User Guide

Version 1.8 | Release Date (December 2014) | 3725-69804-004/A

Polycom® RealPresence® Capture Server, Virtual Edition

Copyright© 2014, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.

All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

System Overview 7
Capacity 7
RealPresence Capture Server Stand-alone Unicast Live Streaming andVoD 9
RealPresence Capture Server and External Stream Servers 10
Multi-user Login Capacity 10
Local Media Storage Capacity 10

User Interfaces 11
Web-based Admin Portal 11
User Permissions through Admin Portal 12
Web-based User Portal 12
Search and Refresh Lists 13
TV user interface (also called the “TVUI”) 13
Understand the Main Menu 13
Console 14

Hardware Installation 15
Hardware Requirements 15

Software Installation 17
Software Requirements 17
Resource and License Management 17
Web Browser and OS Requirements 18
Set up RealPresence Capture Server in a Virtual Environment 18
Configure NFS (Required) 19
Product Activation 20
Obtain the Product Activation Key from Polycom 20
Activate Product and Check the Activation Status 20

System Initialization 22
Configure IP Settings through Console 22
Configure IP Settings through Admin Portal 23
Configure the IP Parameters 23

System Administration 27
Check System Status on Home 27

Signaling Connection 27
System Information 28
System Alerts 28
Signaling Server Status 28
Hardware Status 28
Web Connections 28
External Server Status 29
Manage Users and Groups 29
User Roles 29
Add a New User 29
Modify User Information 30
Create and Manage Groups 30
Set Recording Parameters 31
Configure Signalling Settings 32
SIP 33
Configure Port Settings 34
Set the System Time 35
Configure Media Storage Settings 36
Configure Multicast Settings 36
Before You Start 37
Configure Multicast 37
Multicast 37
Multicast of a Live Streaming 38
Install the Certificate in the System 38
Install a Certificate Authority’s Certificate 39
Create a Certificate Signing Request 40
View Certificate Details 41
Remove a Certificate 41
Client Certification 41
Use OCSP to Obtain Revocation Status 42
Configure QoS 42
Configure SNMP 43
Notice about Using Polycom SNMP MIB Files 44
Diagnostics 45
Password Settings 45
UI Customization 46
Customize IVR Information 47
Customizing UI Logo 47
Setup E-mail 47
Portal Settings 48

Record and Playback 49
Configure Templates 49
Configure Recording Templates 49
Configure Transcoding Template 53
Configure VRRs 55
Start a Recording 56
Point-to-point Recording 58
Dial in from Endpoint 58
Record from RMX via Recording Link 59
Change Conference Layout for MCU hosted calls 59
Dial into a VRR to Start Recording 59
Play Back Media Archives 60
Quick Code 61

Live Streaming/VoD 63
Streaming Using Capture Server 63
Streaming Using External Servers 63
Live Streaming 67
Start Live Streaming 68
Multi Live Streaming 68
View Live Streaming Information 68
View Live Streaming Video 68

Media Management 71
Manage Archives 71
View Archive Details 71
Play Back and Download Archives 71
Modify Archives 73
Dynamic Archiving 73
Transcoding 74

Fault Management 76
System Log Configuration 76
Configure Log Settings 76
Log Management 77
Restart and Shut Down the System 77

Upgrade, Backup, Restore, and Migrate 80
System Upgrade and Downgrade 80
Backup and Restore 81

Back Up and Restore Data 81
Configure an FTP Server for Backup 82
Back Up and Restore Archives 82

Manage Archives and Live Streams Using the User Portal 84
Manage Archives and Live Streams Using the User Portal 85
View Live Streams 86

Appendix A – Console Commands 87
Login Console 87
Console Command Descriptions 88
Help 88
Exit 88
Viewing Device Information 88
Reboot Device 88
Power off System 89
Reset Password 89
Reset Admin Password 89
Restore System Configuration 89
Check Disk Space Usage 89
Ping 90
Network Settings 90

Appendix B – Configure External Servers 92
Live Stream Meetings to an External Media Server 92
Configure the Wowza Media Server 93
Configure the IIS Media Server 95
Configuring the Windows Media Server 99
View the Streaming through External Media Server 100

Appendix C – Configure the Server Working with VCS 102
Configure VCS Calling 102
Configure VCS for SIP Calling 102

System Overview

The Polycom® RealPresence Capture Server is a streaming and recording system that participates in standards-based video and telepresence calls that can be used alone or as an integrated component of Polycom Video Content Management solution. As a native part of the Polycom RealPresence Platform, the RealPresence Capture Server records, archives, and streams telepresence and video conferences for playback on a variety of client devices including tablets, smart phones, desktop computers, and standards-based video endpoints.

The RealPresence Capture Server is typically deployed as part of a larger Polycom RealPresence Platform solution, but it can be used as a standalone solution or with third-party systems. The Real Presence Capture Server's full potential can best be realized when it is integrated with the Polycom RealPresence Media Manager.

By leveraging RealPresence Capture Server with existing telepresence systems, video conferencing endpoints and video infrastructure, or familiar unified communications (UC) tools, your organization can easily convert real-time conferences and events into reusable multimedia assets. Following are some features of RealPresence Capture Server:

- It integrates with Polycom endpoints, conference platforms, and other standards-based video endpoints for automated recording and playback.
- It supports H.323 and SIP standards for interoperability with third-party conferencing systems.
- It is available with several licenses that control the number of video calls that can be recorded, and of those calls, the number of calls that can be streamed live for viewing on web browsers.
- It can output a maximum stream (live or video on demand) of 1080p HD (people+content combined)
- It provides access to live and video call archive streams on devices with compatible browsers including PC, MAC, iOS, and Android devices.
- It enables you to access video call archives via any standard-based endpoint.
- It provides REST API support for third-party integrations.

Capacity

The license that you buy determines the RealPresence Capture Server capability. The following table shows the maximum capacity of the RealPresence Capture Server when it performs different features.

RealPresence Capture Server Capacity

Feature	Description	Maximum Record Port 6 port license
Signaling Connection (H323/SIP)	Specify the maximum number of devices connected to RealPresence Capture Server simultaneously. Connection type: live streaming recording, recording only, and playback.	6
Conference Recording	Specify the maximum number of conferences that can be recorded simultaneously. Connection type: recording only.	6
Single-point Conference Live Streaming	Specify the maximum number of single-point conferences that can be live streamed simultaneously. **Note:** The conference being live streamed can also be recorded.	3 (720p and 1080p)

RealPresence Capture Server Capacity

Capture Server Model	# of Live Ports (720p)	# of Recording/Playback Ports
Recording Only	0	40
Minimum	3	6
Medium	6	12
Maximum	9	18

- Capture Server 40/0 is not licensed to include live unicast/multicast streaming. For 40/0 model, P2P and Quick Code playback features are not available since no live streaming ports are provided. Therefore there is no 1080p live streaming with the product. This is working as designed.
- Capture Server is conducting multiple functions simultaneously: real time decoding/encoding, P2P recording, and Quick Code playback all occupy live streaming ports.
- The models are defined/tailored per RSS5000 hardware. Ports are calculated with a 720p30 baseline profile video plus content.

Live Streaming Resources Usage

The combination of frame rate, resolution and number of live streaming rates used affects the quantity of resources required on the RealPresence Capture Server to support live streaming.

On Capture Server, streaming port calculation is used as quantitative indicator of live streaming resources, one stream (single bitrate) of 720p live streaming costs system resource calculated as one streaming port, for example, one stream of 1080p live streaming needs two streaming ports.

If multiple bitrates are configured for one live stream, each bitrate is calculated separately.

If WMV is configured as the output format and the layout is set as dual window, then one additional port is calculated as well for each bitrate.

In addition to live streaming, the following features also use streaming ports:

- Video call playback

  For details, refer to Video Call Playback.
- Point-to-point recording

Streaming ports are reserved before calls are connected by call rate in recording template.

If there are not enough streaming ports available in system for one service request, the request will be rejected. If real call rate is lower than the call rate configured in recording template, the Capture Server system will update the streaming ports that are really occupied. If system finds that multiple live streams are at the same rate, it will turn off duplicated live rates to save live streaming resources and occupied streaming ports will be updated together. If external live media server is configured in the VRR template, system will not turn off duplicate live rates.

Resource Consumption

Feature	Resources Consumed		
Recording/Live Streaming resource consumed	**Resolution**	**Recording Port**	**Live Streaming Port**
Conference Call (or Endpoint Call)	4CIF/SD	1	0.5
	720p	1	1
	1080p	1	2
Video Call Playback	4CIF/SD	1	0.5
	720p	1	1
	1080p	1	2
P2P	4CIF/SD	1	0.5
	720p	1	1
	1080p	1	2

RealPresence Capture Server Stand-alone Unicast Live Streaming and VoD

RealPresence Capture Server base system is licensed for 250 simultaneous viewing of live and VoD streams from the User Portal. RealPresence Capture Server system supports a maximum number of simultaneous live, or VoD streams, from the User Portal is 500, with the purchase of a stream upgrade option.

Stream Rate on User Portal	Number of Simultaneous Streams from Capture Server User Portal	License	Upgradeable to Maximum Simultaneous Streams
128 kbps–512 kbps	250 streams	Included with base system	500
768 kbps–1728 kbps	125 streams	Included with base system	250
2560 kbps	50 streams	Included with base system	100

Multi-user Login Capacity

The maximum number of Admin Portal session and User Portal session (including anonymous login) is as follows:

- Admin Portal Session: 200
- User Portal Session: 3000

Local Media Storage Capacity

Each 60 minutes 512k call to RealPresence Capture Server requires about 450M storage (the 512k call raw + the default mp4 VoD). For 1024k, the storage space is about double, which is 900M. You cannot calculate an accurate ratio because the size also depends on the video quality.

Storage Usage

Situation	Primary Rate	Call Duration	Storage Space (WMV)	Storage Space (MP4)
1*1080p	1024 kbps (MP4) 1728 kbps (WMV)	60 minutes	~1.4 GB	~870 MB
1*1080p	4096 kbps	60 minutes	~3.2 GB	~3.5 GB
1*720p	4096 kbps	60 minutes	~3.2 GB	~3.5 GB
1*720p	1024 kbps	60 minutes	~862 MB	~860 MB
1*4CIF	512 kbps	60 minutes	~458 MB	~459 MB
1*CIF	128 kbps	60 minutes	~100 MB	~103 MB

	People Video	Content Video
Call Protocols	H.323, SIP	H.239, BFCP (TCP only)
Audio Protocols/Codes	G.711, G.722, G.722.1, G.722.1.C, G.729A, Siren 14 (Mono, Stereo), Siren 22 (Mono, Stereo), Siren LPR, Siren LPRStereo	N/A
Video Codecs	H.264 BP, H.264 HP, H.263, H.263+, H.261	H.264 BP, H.264 HP, H.263, H.263+
Video Resolutions	1080P, 720P, 4CIF, CIF	H.263: XGA (30) H.264: 720P30

Approximate Capacity of Polycom Capture Server 1.7 in Hours of Recording

Resolution	Call speed (Kbps)	Approx. file size of 1 hour @MP4, in MB (from Admin Guide)	Approx. number of hours of recording/TB of storage	Approx. capacity of Capture Server Appliance Local storage, in hours (Capacity=3.5 TB)
CIF	128,000	103	9,700	33,950
4CIF/SD	512,000	459	2,170	7,595
720p30	1,024,000	860	1,160	4,060
1080p30	1,024,000	870	1,140	3,990
720p30	4,096,000	3,500	280	980
1080p30	4,096,000	3,500	280	980

- These values are all estimates because file size varies by call speed, video quality, and amount of motion. File size info from Admin Guide, capacity is per data sheet.
- Storage capacity can be expanded on appliances by using NAS storage.
- Capture Server Virtual Edition uses NAS storage exclusively.

User Interfaces

RealPresence Capture Server provides four interfaces that are used for specific purposes: Web-based Admin Portal, Web-based User Portal, TV User Interface, and Console.

Web-based Admin Portal

This section introduces how to access the web-based Admin Portal and its fundamental layout. You can access the Admin Portal via a compatible web browser and do the following:

- Configure the system.
- Set up recording parameters.
- Monitor system use and health.
- Dial out to endpoints to record meetings, disconnect calls in progress, and create different transcoded versions of archived calls.
- Download media files and give admin users a quick way to access and play archives and live streams.

RealPresence Capture Server system allows up to 200 users with admin rights to log in to the Admin Portal at the same time.

Polycom now offers a virtual edition of the RealPresence Capture Server system, this edition is packaged as an Open Virtualization Archive (OVA) file. The OVA file contains the RealPresence Capture Server application and information about its virtual machine environment. It can be installed as a virtual instance on a host machine running VMware vSphere.

User Permissions through Admin Portal

You can log in to the Admin Portal as an administrator, an auditor or an user. The following table explains user permissions.

User Permissions

Content	Auditor	Administrator	User
Accessible information	System logs	All pages	Archives and live streaming.
Operation permissions	View and download system logs.	View, edit, and delete	Access archives, view live streaming and make recordings.

To log in to the Admin Portal:

1 In the address line, enter the system's IP address in this format: https://<system IP address>/admin.

When an IPV6 address is used, refer to the following format:
`https://[ipv6]/admin`

2 Enter your user name and password to log in to the system.

To enhance security, Capture Server has changed the default from http to https. Request to RealPresence Capture Server system, sent to http://<system IP address>/admin> will be automatically redirected to https://system IP address/admin, for example, https://10.11.12.13/admin.

Using the HTTPS protocol ensures that the configuration of all login credentials (such as user names and passwords) are transmitted using an encrypted channel. This includes those credentials used to communicate with third-party systems on your network. Using the HTTPS protocol limits the ability of anyone monitoring traffic on the network to discover these credentials.

Web-based User Portal

Accessed via compatible device/web browser (PC/MAC, iOS and Android), the User Portal offers the following functions:

- Find, navigate, and search items.
- Play archives and live streams.
- Make calls.

Search and Refresh Lists

You can search items listed on the User Portal, for example, archives and live streaming.

To search for a target item in the list:

» Enter the name, or part of the name of the entry you want to find in the text field, and then click .

- Keyword search is not case sensitive.
- In the archives search box, you can also type the keywords specified to an archive.
- If you want to return to the full list view, delete all characters in the text field and click .

To refresh the list:

Click the icon displayed above the list.

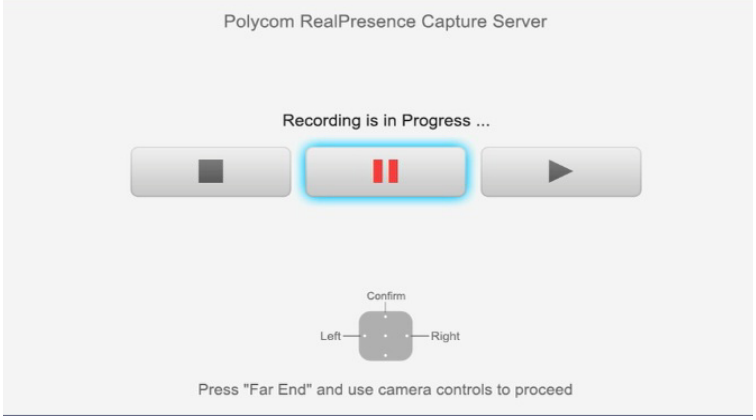
TV user interface (also called the “TVUI”)

Accessed via standards-based video conferencing endpoints, this interface can be used to record meetings, control recording and playback.

Understand the Main Menu

In addition to the Admin Portal, the RealPresence Capture Server system also provides a TV user interface for you to perform the most commonly used operations. The TV user interface appears after an endpoint dials the RealPresence Capture Server system and sets up a connection successfully.

TV User Interface



After the endpoint sets up connection with the RealPresence Capture Server system, it enters the TV user interface menu page, where common recording and playback options are provided, as shown below.

If the **Start Recording Immediately** function has been enabled in the VRR used by the endpoint for dialing, the endpoint enters **Recording Status** directly. You can control the RealPresence Capture Server system using the FECC and DTMF functions of the remote control. When your endpoint supports FECC or DTMF, use the remote control to operate the TV user interface menu page.

The table below defines in detail the FECC and DTMF operation keys on the remote control of Polycom endpoint.

FECC and DTMF Operation Keys

Scenario	FECC	Description	DTMF	Description
When in the menu display state		Pause the recording.	*1	Pauses the recording.
		Confirm the selection.	*2	Starts or resumes a paused recording.
		Select leftward (cyclic).	*3	Stops the recording.
		Select rightward (cyclic).	*5	Plays back the recording.

When in the video playing state	-	-	*1	Pauses the current video.
	-	-	*2	Starts or resumes a paused video.
	-	-	*3	Stops playback of the current video and returns to the main menu.
	-	-	*4	Reverses the current video.
			*6	Fast forwards the current video.

Console

Accessed via vSphere client console or SSH, console is used to view/change IP settings and reboot the system. For example, set DNS server, view disk space usage and shut down the system.

Refer to AppendixA for more supported command line information.

Hardware Installation

The front panel of the Polycom RealPresence Capture Server system is shown in the next illustration.

Hardware Requirements

The following table shows the hardware requirements for the RealPresence Capture Server.

Hardware Requirements

Simultaneous Recording Ports	**6**	**12**	**18**	**40**
LIVE Stream	**3**	**6**	**9**	**0**
Virtual Cores	8+	12+	16+	8+
CPU	• 2.67GHz (Intel® Xeon® CPU x5650@ 2.67GHz or better) CPU • 2.90GHz (Intel Xeon CPU E5-2690 @ 2.90GHz or better) CPU	• 2.67GHz (Intel® Xeon® CPU x5650@ 2.67GHz or better) CPU • 2.90GHz (Intel Xeon CPU E5-2690 @ 2.90GHz or better) CPU	• 2.67GHz (Intel® Xeon® CPU x5650@ 2.67GHz or better) CPU • 2.90GHz (Intel Xeon CPU E5-2690 @ 2.90GHz or better) CPU	• 2.67GHz (Intel® Xeon® CPU x5650@ 2.67GHz or better) CPU • 2.90GHz (Intel Xeon CPU E5-2690 @ 2.90GHz or better) CPU
Minimum RAM	16 GB	16 GB	32 GB	32GB
Minimum Accessible Storage	80 GB	120 GB	120 GB	120 GB
Software Requirements	**VMWare vSphere 5.1/5.5**	**VMWare vSphere 5.1/5.5**	**VMWare vSphere 5.1/5.5**	**VMWare vSphere 5.1/5.5**

Please ensure sufficient CPU and memory resources are reserved for VMware as required on the table, otherwise the system may not function properly or in the worst case may fail to respond.

Software Installation

Software Requirements

RealPresence Capture Server - Virtual Edition is supported on VMware vSphere 5.1/5.5. Before you install and configure the RealPresence Capture Server system, you need the following:

- VMware vSphere 5.1/5.5 client installed where you can access the ESXi host
- Login credentials and IP addresses of one or more VMware vShpere hosts on which you will deploy your RealPresence Capture Server OVA
- A web browser where you access the Viewer Portal. See table "User Portal Web Browser Requirement" for the supported versions

Resource and License Management

For the 1st installation of Virtual Edition, the 90-day trial license provides 6/3 capacity and basic functions. To permanently enable the Capture Server system and enjoy the full capabilities, a RealPresence Capture

Server license is required. For this release, the 6/3 model is supported for Virtual Edition only, which is different from the Appliance Edition.

Licence of Capability

License
6 Calls Record 3 Calls (of the 6 total calls) stream live

Web Browser and OS Requirements

The following table lists the requirements on your computer to access the Admin Portal and User Portal.

User Portal Web Browser Requirement

Operating System	Browser Name	Version
PC (Windows 7, and Windows 8)	Internet Explorer	9, 10, 11
	Firefox	32, 33
	Chrome	38, 39
MAC OS-X (Intel-based Leopard, Snow, and Lion)	Safari	7.1, 8.0
	Firefox	32, 33
	Chrome	38, 39
iOS 7, 8	Safari	7.1.2, 8.1.1
Andriod phone and tablet	Android browser	4.3, 4.4.2

Set up RealPresence Capture Server in a Virtual Environment

The following steps assume you are familiar with deploying applications into a VMware environment.

For more information about deploying applications into a VMware environment, see VMware website.

To set up RealPresence Capture Server in a virtual environment:

1. Obtain the RealPresence Capture Server OVA package.
2. Deploy the OVA file into the VMware vShpere hosts that you have set up.

If the VMware vSphere host is very busy or it does not match the RealPresence Capture Server hardware requirements, the deployment may fail. See table "Hardware Requirements" for more about hardware requirements.

3. From the vSphere client, edit the instance and configure to the customer options.
4. Click the **Summary** tab and note the temporary IP address of RealPresence Capture Server system assigned by DHCP.
5. On VMware console, click **Edit** and adjust the CPU, memory, and the minimum disk space.

Configure NFS (Required)

Capture server virtual edition requires a NFS share as its media storage. The procedure below demonstrates how a NFS share is configured on a typical Linux distribution.

Make sure that NFS is co-located on the same switch/location as the Capture Server system to ensure stable I/0 operations.

To export a shared storage location via NFS on a typical Linux system, CentOS used in below example:

1. Make sure the NFS service has been installed and is running.

   Examples:

```
[root@centos-nfs ~]# service nfs status
rpc.svcgssd is stopped
rpc.mountd (pid 20129) is running...
nfsd (pid 20194 20193 20192 20191 20190 20189 20188 20187) is running...
rpc.rquotad (pid 20125) is running...
```

2. Edit the NFS configuration file /etc/exports to set the file system paths for export.

   Examples:

```
[root@centos-nfs ~]# cat /etc/exports
/home/nfs *(rw,no_root_squash)
/home/nfs_zip_1 192.168.9.78(rw,no_root_squash)
```

3 Restart the NFS service.

Examples:

```
[root@centos-nfs ~]# service nfs restart
Shutting down NFS daemon:                                  [  OK  ]
Shutting down NFS mountd:                                  [  OK  ]
Shutting down NFS quotas:                                  [  OK  ]
Shutting down NFS services:                                [  OK  ]
Starting NFS services:                                     [  OK  ]
Starting NFS quotas:                                       [  OK  ]
Starting NFS mountd:                                       [  OK  ]
Stopping RPC idmapd:                                       [  OK  ]
Starting RPC idmapd:                                       [  OK  ]
Starting NFS daemon:                                       [  OK  ]
```

4 Go to **Configuration > Media Storage Settings** and configure the settings.

Product Activation

Obtain the Product Activation Key from Polycom

A new installation of RealPresence Capture Server Virtual Edition comes with a 90-day trial license. You must activate the license shipped with your order with the product serial number (you can find this by choosing **Admin > Product Activation)** identified within RealPresence Capture Server.

To obtain the product activation key:

1 Go to **Admin > Product Activation** to obtain the serial number. Write it down for later use.

2 Enter the following web site address in the address bar of the web browser: support.polycom.com. and go to **Support Home**.

3 Go to **Licensing & Product Registration > Activation/Upgrade**.

4 Click **All other Polycom Products** in the pop-up window.

5 Enter your e-mail address and password to log in to or register for a new account.

6 Follow the page prompts step by step to generate the Key Code required for system activation.

7 Enter the **Serial Number** you recorded and click **Next**.

8 Follow the page prompts step by step to generate the Key Code required for system activation. Enter the product options license numbers.

9 Note down the activation key (Key Code) on the page and click **Upgrade**.

10 Go back to Capture Server Admin Portal and activate the system under **Admin > Product Activation**.

To download Capture Server software and VE version:

1. Go to **Admin > Product Activation** to obtain the serial number. Write it down for later use.
2. Enter the following web site address in the address bar of the web browser: support.polycom.com. and go to **Support Home**.
3. Go to **DOCUMENTS & DOWNLOADS > UI Infrastructure**.
4. Click **Video Content & Management Solutions** at the left side bar.
5. Click **Polycom RealPresence Capture Server, Virtual Edition**.
6. Enter your e-mail address and password to log in to or register for a new account.
7. Click the EULA and agree to it.
8. Click **Submit**.
9. Go to Capture Server Admin Portal and activate the system under **Admin > Product Activation**.

To view the system activation status:

» Go to **Admin > Product Activation**. The following system information is displayed.:

Parameter	Description
License Type	Permanent license or 90-day trial version
Software Version	Current version of the software running on the system
Serial Number	Product serial number
Activation Status	Whether the system is activated; indicates activated system, and indicates it is not activated
Max Recording Ports	Maximum number of recording ports supported by the system
Max Live Streaming Ports	Maximum number of live streaming ports supported by the system
Max Streaming Sessions	Maximum number of video-on-demand and live streaming sessions supported by the system. Base: 250. Note: After purchasing and activating the license, the streaming sessions capacity will be increased from 250 to 500.
Media Encryption	Whether the AES encryption function of the system is activated. This is a charged function. You can use it only after purchasing the license and activating it.
Streaming without recording (no archive)	Whether the streaming without recording function of the system is activated. Once this function is activated, the system performs live streaming without recording and no archives left.
Timecode Watermark	Whether the basic timecode watermark capability for transcoded mp4 on-demand files is activated. On-demand archives can be output with basic timecode watermarking.

System Initialization

Fast Configuration Wizard

The Fast Configuration Wizard pops up if **Media Storage Settings** is not configured, it gets you up and running as soon as possible, all settings in the wizard can be changed later on under the various configuration pages.

Step 1: Configure Media Storage Settings

By default, RealPresence Capture Server stores the files on a network file system if you enable it.

For configuration steps, refer to Configure Media Storage Settings.

Note: You need to click **Next** and save changes at the next step by clicking **OK**, otherwise the configured settings will not be saved.

Step 2: Configure IP Settings

The RealPresence Capture Server system supports both IPv4 or IPv4 & IPv6 network communications. You can configure parameters to be used for network communication, including system IP address, DNS server, and NAT server.

For configuration steps, refer to To set IP:.

If you are done with configuration, click **OK** to save the changes.

Step 3: Product Activation

The basic system information is displayed here

For configuration steps, refer to Product Activation. As the Virtual Edition comes with a 90-day trial license, you can use the Capture Server system without activating the license.

Step 4: Configure Signaling Settings

For H.323, if a gatekeeper is configured on your network, you can register RealPresence Capture Server to the gatekeeper to simplify calling. A gatekeeper manages functions such as bandwidth control and admission control. A gatekeeper also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.

If you make SIP calls, you can register RealPresence Capture Server to a SIP server to simplify calling.

For configuration steps, refer to Configure Signaling Settings

Step 5: Configure System Time

You also can set the RealPresence Capture Server system time from the Fast Configuration Wizard

For configuration steps, refer to Set the System Time

Configure IP Settings through Console

By default, when a new RealPresence Capture Server is started, it obtains an IP address from the DHCP server automatically. Follow the steps below to check the IP address assigned by DHCP server. You can configure IP settings from either Capture Server system's Console or Admin Portal.

To set the system IP address in the RealPresence Capture Server's console:

1. Open the console of your RealPresence Capture Server.
2. The default console display is shown in the next illustration

Polycom
Polycon RealPresence Capture Server
Copyright 2010-2013 Polycom, Inc. All Rights Reserved.
Device Network Information:
eth0[192.168.1.254]
eth1[]
Use a supported browser to configure/manage this Polycom RealPresence Capture Server:
http://192.168.1.254
Use a supported telnet client to configure/manage this Polycom RealPresence Capture Server:
192.168.1.254

3. The IP address displayed on console is shown in the above illustration, the default IP address is **https://192.168.1.254**
4. If needed, modify the RealPresence Capture Server IP address in the Admin UI. See To change the system's initial IP settings from the Admin Portal:
5. Type **Alt+F2** keys to go to the login screen.
6. Enter the user name and password (both are ***polycom*** by default).
7. Set RealPresence Capture Server a static IP or DHCP for LAN interface using `Network Settings` command, refer to Network Settings for details.

   Note: After you are finished with DHCP setting configuration, go to console and get the IP address information assigned by DHCP server.
8. After you set the IP, the Capture Server system will ask if you want the changes, click **Yes** to reboot.

Configure IP Settings through Admin Portal

The RealPresence Capture Server system supports both IPv4 or IPv4 & IPv6 network communications. You can configure parameters to be used for network communication, including system IP address, DNS server, and NAT server.

The RealPresence Capture Server system supports IPv6 system management.

To set IP:

1 Go to **Configuration > IP Settings** and configure the following settings:

Set IP Parameters

Parameter	Description
Enable Network Separation	Select this check box to route the management, streaming traffic and video call traffic through LAN 1 and LAN 2 interfaces separately. This offers higher security for the signaling data.
Obtain an IP Address Automatically (DHCP)	If you select this radio button, RealPresence Capture Server obtains an IPv4 address automatically via DHCP. **Note:** Obtaining an IP address automatically is not recommended. For best results, assign a static IP to RealPresence Capture Server.
Using the following IP Address	• **IP Address:** the IP address of the system. • **Subnet Mask:** the subnet mask of the system. • **Default IPv4 Gateway:** the address of the interface to use for accessing the IPv4 gateway. • **Preferred DNS Server:** the preferred DNS server address for the system to resolve domain names. • **Alternate DNS Server:** the alternate DNS server address for the system to resolve domain names.
Enable IPv6	Specify whether to enable IPv6 related functions.
Obtain an IP Address Automatically (IPv6)	Specify whether to obtain the IPv6 address automatically using Stateless Address Auto-configuration (SLAAC). **Note**: Obtaining an IP address automatically is not recommended. For best results, the system should be configured with a static IP address.
Using the following IP Address (IPv6)	Select this option to manually configure a static IPv6 address: • **Link Local Address**: Specify an address for link local communication. Routers do not forward packets with link local addresses. • **Site Local Address**: Specify an address for site local communication. Routers do not forward packets with site local addresses. • **Global Address**: Specify one or several address for communication with external IPv6 networks. Separate several addresses with a comma (,). • **Default IPV6 Gateway:** Specify the address of the interface to use for accessing the IPv6 gateway.

Enable ICMP V6 DAD	Specify whether to enable Duplicate Address Detection (DAD) to ensure the IPv6 address set to the system is unique in the local network.
Enable ICMP Echo	Specify whether to allow the system to respond to an ICMP (Internet Control Message Protocol) echo request (Ping) sent from other devices in the network. In some high-security environments, you may need to disable this option to protect the system from Ping attacks.
MTU	Specify the Maximum Transmission Unit (MTU) size.
LAN Speed	Specify the speed or duplex modes for the LAN port. Select **Auto** to let the system set the speed automatically. **Note:** When setting the LAN port speed, contact your network administrator to ensure that the switch link rate matches the system port speed.
NAT Public (WAN) Address	Set the external IP address in Network Address Translation (NAT) environment. NAT environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices outside the LAN to access Capture Server Web Portal, view live streaming or VoD playback.

2 Configure the following general settings:

General System Network Parameters

Parameter	Description
Host Name	Specify the host name of the system.
Domain	Specify the domain name of the system.

3 Click **Add** to add static routes. You need to enter the following information for each route:

Set Route Parameters

Parameter	Description
Destination	Specify the IP address of the destination network.
Gateway	Specify the IP address of the gateway to access the destination network.
Subnet Mask	Specify the subnet mask for the destination network.

4 Click **OK**. The system restarts to apply your changes.

System Configuration

This section explains the functions used for system administration in detail.

Check System Status on Home

You can find real time system status and information on Home.

Signaling Connection

Shows connection information and recording status of the calls to and from video endpoint or MCUs with this Capture Server. Click to expand detailed parameters information. The table below provides parameters descriptions.

Signal Connection Parameters

Parameter	Description
Far End Number	The far end number used by the connection.
Start Time	When the calls started.
Signaling Type	H.323 or SIP.
Dial In/Out	Whether the connection is incoming or outgoing.
VRR Number	The VRR number used by the connection.
Live Streaming	Whether the connection is performing live streaming.
Detail	Additional information like VRR name, audio type, audio call rate, video type, video call rate, etc.
Real Time Information	Displays call address, audio packet loss, video resolution, video frame rate, etc.

You can control the recording using the controls:

- : Start recording.
- : Pause recording.
- : Resume recording.
- : Stop recording.
- : End the connection.

  You can dial out to connect the endpoint to record using **Dial out to record**.

You can control the Quick Code playback using the controls:

- : Pause playback.
- : Resume playback.
- : Stop playback.
- : Start playback.
- : Fast backward playback.
- : Fast forward playback
- : End the connection.

You can control the RMX playback using the controls:

- : Pause playback.
- : Resume playback.
- : Stop playback.
- : Fast backward playback.
- : Fast forward playback
- : Change conference layout
- : End the connection.

System Information

Displays following system basic information:

- System name
- The current version of the software running on the system.
- The maximum number of recording ports and live streaming ports supported by the system.
- Recording ports and live streaming ports usage.

System Alerts

Shows the system alert information, for example, registration to primary gate-keeper failed, LAN2 failed to acquire DNS automatically, IP address conflict for LAN1, CPU usage is too high, memory usage is too high, NFS connection is lost, temperature is out of range, log size has reached the threshold value, etc.

Signaling Server Status

Displays gatekeeper registration status and SIP server registration status. When the H.323 registration is successful, the system's E.164 prefix and H.323 alias are displayed.

Hardware Status

The following table shows the indicators and the hardware status in general.You can check the following status:

- **Basic**

  - **CPU Usage**
  - **Memory Usage**
  - **System Disk Usage**
- **Extension:** Specifies value, total storage and status for RAID, disk, local media disk, power, etc.

Web Connections

Displays connection status on both Admin and User Portal for administrators, users, auditors, and anonymous users.

- **Admin Portal Connections:**
  - **Current Administrators**
  - **Current Users**
  - **Current Auditors**
- **User Portal Connections:**
  - **Current Administrators**
  - **Current Users**
  - **Current Anonymous**

External Server Status

The system can be integrated with external servers, such as IIS and WOWZA. You can check the configuration for IIS, WOWZA, Windows Media Server, AKAMAI, AD server and NFS server respectively.

Note: Make sure the NFS server is set up beforehand.

Manage Users and Groups

This section explains how to manage users.

User Roles

Users who are defined in the RealPresence Capture Server system can log in to the system's Admin Portal to complete authorized operations. The system supports three user roles:

- Auditor: Who can only audit and manage system logs and set personal information.
- Administrator: Who can perform the most operations, and can view and configure all pages.
- User: Who can access archives and view live streaming.

Add a New User

You can add a local user to the system.

To add a local user:

1. Go to **User > Users**.
2. Click **Add**.

3 Configure the following settings (* indicates mandatory options):

Adding an User

Parameter	Description
User ID	Specify the user ID used for web login. User ID must be unique with a length of 1-128 characters, and consist of alphanumeric or "_" symbol characters. Once created, user ID cannot be modified.
Full Name	Specify the user's full name.
Password	Specify the login password.
Confirm Password	Specify the confirmed password which must be identical to the login password.
Role	User roles: **Administrator**, **Auditor** or **User**. Different roles determine the user operation permissions after logging in to pages.
Description	Specify additional related information.

Modify User Information

The administrator can modify local user information and password, or delete user.

To modify user information:

1 Go to **User > Users**.
2 Select the user entry you want to edit.
3 Click **Edit**.
4 Enter the user information, and then click **OK**.

To modify user password (local user only):

1 Go to **User > Users**.
2 Select the user entry you want to modify.
3 Click **Change Password**.
4 Enter the new password and confirm password, then click **OK**.

After the password is changed by the administrator, the user is required to change the password when he logs in to the system using that password for the first time.

To delete a user:

1 Go to **User > Users**.
2 Select the user entry you want to delete.
3 Click **Delete**.

Create and Manage Groups

You can create user groups and set permissions for groups.

A default group, named all-users, is built in the system. It includes all the users defined in the RealPresence Capture Server system. all-users group cannot be modified or deleted. Administrators can define a new group, modify or delete existing groups.

To view user groups:

1. Go to **User > Groups**.
2. Filter by **Local Groups** or **AD Groups.**

To create a new user group:

1. Go to **User > Groups**.
2. Click **Add**.
3. Specify a name for the group. The group name must be unique. You can enter associated descriptions if necessary.
4. Click **Group Members**.
5. Select users to add to the group, and then click **Add**.

   To delete an item, select it and click **Delete**.

To modify or delete an existing group:

1. Go to **User > Groups**.
2. Select the group entry you want to delete.
3. Click **Edit** or **Delete**.

Set Recording Parameters

You can configure supplementary recording settings from **Configuration > Call Settings**. The system call setting will be applied as default value to all calls in the system. If there is difference in recording template, then usually recording template setting will take precedence.

To configure recording setting options:

1. Go to **Configuration > Call Settings**.

2 Configure the following settings:

Record Parameters

Parameter	Description
Allow recording even when no resources are available to create live stream(s).	If this option is selected, when there are insufficient resources available to live stream a meeting, the system records the meeting to the hard disk automatically. You cannot continue viewing the video in real time through the web. However, you can play back the video upon the completion of recording and format conversion. If this option is not selected, when there are no live streaming resources, the system rejects all calls that have live streaming enabled.
Key Frame interval	Specify the fast forward and backward intervals when playing back recorded files on an endpoint. For example, if it is set to one minute, the system inserts an index marker every minute when recording. When you press **Fast forward** using FECC (Far End Camera Control) or DTMF, the video playback jumps to the nearest index marker from the current location. Shorter intervals result in larger archive.
Indication Tone	Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second.
Media Encryption	If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled and SIP connections: • **Required For All Calls:** Enable the AES encryption for all H.323 and SIP calls, including video and audio only calls. This option requires the device to connect the system with AES enabled, otherwise, the connection cannot be set up. • **When Available**: Enable the AES encryption and SIP connections when the peer device enables the AES option, and vice versa. • **Off:** Disable the AES encryption and SIP connections.
Support AES 256-Bits key for encryption	If the Capture Server is licensed for call encryption, this option specifies whether to enable the 256-bit key for AES encryption. If not selected, the AES uses 128-bit key for encryption by default.
Max Call Length	The maximum call length for recording calls. The value is 4 hours by default. Note: Valid call length ranges from 1 to 8 hours.
Max Call Length (for streaming only call)	The maximum call length for streaming only calls. The value is 8 hours by default. Note: There is no limitation to this option.
Enable all IVR notifications	Enable IVR service at system level, the default left time to play IVR is 10 minutes
Enable Global Quickcode Playback PIN	Enable quickcode playback PIN at system level. Note: If a PIN code is set under archive properties, the individual PIN code will override that set at system level.

Note: The template value will override the system value set under **Configuration > Call Settings** on Admin Portal.

Configure Signaling Settings

For H.323, if a gatekeeper is configured on your network, you can register RealPresence Capture Server to the gatekeeper to simplify calling. A gatekeeper manages functions such as bandwidth control and admission control. A gatekeeper also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.

If you make SIP calls, you can register RealPresence Capture Server to a SIP server to simplify calling.

H.323

If your network supports H.323, you can register RealPresence Capture Server to a H.323 server to simplify calling.

To register the system to a gatekeeper to make H.323 calls:

1. In the address line, enter the system's IP address in this format: https://<system IP address>/admin.
2. Go to **Configuration > Signaling Settings > H.323**.
3. Select **Register To Gatekeeper**.
4. Configure the settings listed in the following table. After you finish the configuration, click **OK**.

H.323 Gatekeeper Parameters

Parameter	Description
Gatekeeper type	Choose between **Polycom** and **Cisco VCS**.
Primary Gatekeeper	Indicates whether the system is registered to the primary gatekeeper.
Gatekeeper Address	Specify the IP address for the gatekeeper. Note: Never enter Capture Server's IP address.
Gatekeeper Port	Specify the port number for the gatekeeper, the default value is 1719.
Register User Information for Gatekeeper	Specify whether to register the system to a Polycom Gatekeeper server for H.235.0 authentication. When H.235.0 authentication is enabled, the gatekeeper ensures that only trusted endpoints are allowed to access the gatekeeper.
Gatekeeper User	Specify the user name for registration with the Polycom Gatekeeper server.
Gatekeeper Password	Specify the password for registration with the Polycom Gatekeeper server.
Alternate Gatekeeper	Indicates whether the system is registered to the alternate gatekeeper. **Note**: The alternate gatekeeper is used only when the primary gatekeeper is not available.
System Prefix / E.164	Specify the E.164 number for the system.

System H.323 Alias	Specify the H.323 alias for the system.
Remote Display Name	Specify the name to be displayed to the far end. Note: If you set the remote display name with dual-bytes characters like Chinese, you will not see the characters on the far end endpoints in a H.323 call between endpoints and the Capture Server system.

If the RealPresence Capture Server is registered to DMA as gatekeeper, you can find Capture Server's information on DMA portal under **Network > MCU > MCUs**.

SIP

If your network supports SIP, you can use SIP to connect video calls. RealPresence Capture Server supports SIP integration with SIP servers such as the Polycom DMA.

To configure the SIP settings:

1. Go to **Configuration > Signaling Settings > SIP**.
2. Configure the following settings:

SIP Parameters

Parameter	Description
Transport Type	Specify the transport layer protocol used for communicating with the SIP server. It needs to be consistent with the protocol supported by the SIP server.
Enable Certificate Validation	Specify whether to validate the server's certificate before accepting it. This option is available only after you select **TLS** as the **Transport Type**. **Note**: RealPresence Capture Server always sends its own certificate to the server, regardless of the selection here.
Register to SIP Server	Specify whether to register the system to the SIP server.
SIP Server Type	Choose a SIP server type from the dropdown list, currently only Generic available.
SIP Server status	Specify: • **Server Address** • **Server Port** • **Server Domain Name** Note: Never enter Capture Server IP for **Server Address**.
Register User's Information	Specify: • **User Name** • **Auth User Name** • **User Auth Password**

Outbound Proxy Server	For communication with the SIP server when the system is configured on the internal network, an outbound proxy server is required to implement traversal of the firewall or NAT. In this case, you need to set the IP address and port number for the outbound proxy server. • **Server Address:** Enter an address of the SIP server. • **Server Port:** Enter the port of the SIP server.

3 Click **OK**.

- If you need to configure both H.323 Gatekeeper parameters and SIP parameters at the same time, click **OK** after you finish the configuration of both parameters.
- If the RealPresence Capture Server is registered to DMA as SIP server, you can find Capture Server's information on DMA portal under **Network > Endpoints**.

Configure Port Settings

Port Settings allow specific ports in the firewall network environment to be allocated to multimedia calls.

To configure the port:

1 Go to **Configuration > Port Settings.**
2 Select **Enable port configuration**.
3 Configure the following settings:

Port Parameters

Parameter	Description
TCP Ports	Specify the TCP port range. You can set the starting port number (the default value is 10000), and the ending port number is calculated automatically.
UDP Ports	Specify the UDP port range. You can set the starting port number (the default value is 20000), and the ending port number is calculated automatically.
Streaming Port	Specify the streaming port range. The default value is 1640.
Multicast Port	Specify the multicast port range. The default value is 1641.

4 Click **OK**. The recording server restarts to apply your changes.

Set the System Time

You also can set the RealPresence Capture Server system time from the Admin Portal.

To set the system time:

1 Go to **Configuration > System Time**.

2 Configure the following settings:

System Time Parameters

Parameter	Description
Time Service	Specify how to set the system time: • **Console**: Synchronize the system time with your computer. • **NTP Server**: Obtain the system time from a time server.
Date	The current system date and time. Changing the time manually is not recommended.
Time	
Time Zone	The current time zone.
The NTP servers 1 and The NTP server 2	Specify the address or domain name of a network time server. NTP server 2 is used only when NTP server 1 is not available. **Note:** If you set a domain name, make sure you have already set a DNS server address that can resolve this domain name in **Configuration > IP Settings**.

3 Click **OK**. The system restarts to apply your changes.

Configure Media Storage Settings

By default, RealPresence Capture Server stores the files on a network file system if you enable it.

To save your files on a network file system:

1 Click **Configuration > Media Storage Settings**.

2 Configure the following settings for the network file system.

Media Storage Setting

Parameter	Description
NFS Server Name	Enter a name for the NFS server.
NFS Server Address	Enter an address of the NFS server.
NFS Storage Folder	Specify the folder path to the NFS storage. Note: Make sure the NFS server is set up beforehand.
Test	Test whether the NFS server is reachable.

Synchronize archives when storage setting changed	When this option is checked, the archives on the storage will be synced up with the archive record in the system database, and could be viewed from portal (viewer or admin). The sync-up action takes effect after the system restarts.
Send warning e-mail to Admin when remaining NFS free space reaches: (GB)	Set a NFS storage space threshold. You can set a value in the range of 10-50GB. After the system reaches the threshold, RealPresence Capture Server will send notifications to specified receivers.

3 Click **OK.** The server restarts to apply your changes.

- If Network storage is disabled or error, RealPresence Capture Server cannot dial in and dial out.
- Capture Server supports NFS Version 2 and 3.

Configure Multicast Settings

The Polycom RealPresence Capture Server system supports the multicast function and can perform the one-to-many transmission of video streams. The system only needs to send the video streams once so that multiple computers can simultaneously share live streaming so as to greatly reduce the demand for transmitting network video streams and save the network bandwidth.

The Polycom RealPresence Capture Server system supports the simultaneous multicast of up to 100 channels.

Before You Start

To use the multicast function successfully, the following conditions are required to be met:

- The multicast function is activated in the Polycom Capture Server system. Contact your supplier to obtain this function.

  The multicast function is disabled by default.
- Routers and switches in the network of client computers are configured correctly to support the IP multicast communication with the Polycom Capture Server system.

Configure Multicast

Before you use the system to perform the multicast, it is necessary to configure parameters on the Multicast page.

To configure multicast parameters:

1 Go to **Configuration > Multicast Settings**.

2 Configure the following settings:

Parameter	Description
Auto Multicast for Live Streaming	If this option is selected, all the live streaming will start multicast automatically. This option is disabled by default.
Multicast IP Pool Starting Address	Specify the initial IP address of the multicast address pool. The system uses 100 consecutive addresses starting with this address to perform the multicast. The valid starting IP address range is 233.0.0.0 - 239.255.255.156.
Multicast TTL.	Specify the TTL value: • **Local Network -- 1** • **Intranet -- 32** • **Internet, Inter-continent -- 64** • **Internet, Inter-continent -- 128** • **Maximum allowed value -- 255 (default value)**

You cannot start or stop the multicasts manually, multicasts will start once the live streaming starts and stop after the live streaming stops.

Multicast

The Polycom RealPresence Capture Server system supports the video multicast function and can send video streams to a group of computers at the same time. Users can play multicast videos from either the system's Admin Portal or User Portal.

Multicast of a Live Streaming

Users can start a multicast from the live streaming list. The system supports up to 100 concurrent multicast channels.

- VoD archive multicast is not supported.
- Streaming format is defined in meeting templates. For more information, see To define a recording template:.

To start a multicast (when multicast is disabled):

1. Create a recording template with **Enable Multicast** selected.
2. Configure **Multicast TTL** from recording template.
3. Create a VRR with the configured recording template.
4. Start a live streaming with the VRR, and multicast starts at the same time.

To view a multicast streaming:

1. Click **Live Streaming**.

2 Select a live streaming and click **Multicast Detail**.

3 Click **Play**

The media file is played ina new window.

- If there are MP4 and WMV streams, there would be two multicasts for the two stream types.
- If there are two bitrate streams, center will choose the higher bitrate stream to do multicast;
- You can view multicasts from either Admin or User Portal.

Certificate Management

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other. The RealPresence Capture Server system supports using X.509 certificates (version 3 or earlier) for authenticating the network connections. Once a certificate is purchased and installed in the RealPresence Capture Server system, it may be used for the following connections:

- Web server (TLS)
- Microsoft Active Directory server (LDAPS)
- SIP recording (TLS)
- FTP Server (FTPS)

Install the Certificate in the System

Certificates and certificate chains are a security technology that allows networked computers to determine whether to trust each other.

By default, to support encrypted communications and establish a minimal level of trust, the system includes a default key and self-signed certificate.

However, to implement a full certificate chain to a root certificate authority (CA), the system requires both a root CA certificate and an identity server certificate signed by the root CA. Therefore, at some time you must request these certificates from your CA.

Install certificates on the RealPresence Capture Server system in Admin Portal

1 Install your chosen certificate authority's public certificate, if necessary, so that the RealPresence Capture Server system trusts that certificate authority.

2 Create a certificate signing request to submit to the certificate authority.

3 Install a public certificate signed by your certificate authority that identifies the RealPresence Capture Server system.

The RealPresence Capture Server system accepts the following types of certificate chains or single certificates:

Certificate Types

Type	Description
.pem	Privacy Enhanced Mail, base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

.cer, .crt, .der	Usually in binary DER form, but Base64-encoded certificates are also common (refer to .pem).
.p7b, .p7c	PKCS#7 SignedData structure with certificates or CRLs and without data.
.p12	PKCS#12, may contain public certificates and password-protected private keys.
.pfx	PFX, predecessor of PKCS#12. This type usually contains data in PKCS#12 format, for example, with PFX files generated in IIS.

Install a Certificate Authority's Certificate

You must install a certificate authority's certificate if you don't obtain a certificate chain that includes a signed certificate for the RealPresence Capture Server system, your certificate authority's public certificate, and any intermediate certificates.

The certificate must be either a single X.509 certificate or a PKCS#7 certificate chain. If it is ASCII text, it's in PEM format, and starts with the text -----BEGIN CERTIFICATE-----. If it is a file, it can be either PEM or DER encoded.

To install a certificate for a trusted root CA:

1. Go to **Configuration > Certificate Management**.
2. If you are using a certificate authority that is not listed, obtain a copy of your certificate authority's public certificate.
3. Select **Install Certificates**.
4. Do one of the followings:
   - Click **Upload Certificate** and click **Add** to browse to the certificate. Upload the selected certificate. Enter your password if necessary.
   - Copy the certificate text, and then click **Paste certificate** to paste it into the text box.
5. Click **OK**. If the certificate can be verified, the system installs it.

Create a Certificate Signing Request

This procedure creates a CSR (certificate signing request) that you can submit to your chosen certificate authority.

Creating a new CSR overwrites the existing pending CSR, if any.

To create a certificate signing request:

1. Go to **Configuration > Certificate Management**.
2. Select **Issue Signing Request**.

3 Enter certificate information:

Certificate Information

Parameter	Description
Common Name	Specify the name of the system.
Organizational unit (OU)	Specify the business unit defined by your organization (Optional). Use a comma(,) to separate several business units.
Organization	Specify your organization's name (Optional).
City or locality (L)	Specify the city where your organization is located (Optional).
State (ST)	Specify the state or province where your organization is located (Optional).
Country (C)	Specify your two-character country code.

4 Click **OK**.

The **Certificate Signing Request** dialog box displays the encoded request.

5 Copy the entire contents of the **Encoded Request** box and submit it to your certificate authority. Be sure to include the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----.

Depending on the certificate authority, your CSR may be submitted by pasting it into a web page.

6 Click **OK**.

When your request has been processed, your certificate authority sends you a signed public certificate for your RealPresence Capture Server system. Some certificate authorities also send intermediate certificates or its root certificates.

The certificate authority might send you the certificate as e-mail text, an e-mail attachment, or content on a secure web page.

Refer to To install a certificate for a trusted root CA:to install a certificate.

View Certificate Details

You can review installed certificate details.

To view the certificate details:

1 Go to **Configuration > Certificate Management**.

2 Click **Display Details**.

Certificate Details

Parameter	Description
Certificate Info	States the purpose and alias of the certificate.
Issue To	States the entity to which the certificate was issued and the certificate serial number.
Issue By	States the issuer.

Validity	States the issue and expiration dates.
Fingerprints	States SHA1 and MD5 fingerprints (checksums) for confirming certificate.

When a certificate is about to expire, you are notified ten days prior to the expiration date.

Remove a Certificate

You can remove installed certificates.

A certificate cannot be removed when it is the only private certificate which can be used as web service certificate in the system.

To remove a certificate:

1. Go to **Configuration > Certificate Management**.
2. Highlight the certificate you want to remove.
3. Click **Delete**.

Client Certification

If client certificate validation is enabled in the system, other systems can connect to the RealPresence Capture Server system only if they present a client certificate issued by a CA that the system trusts.

Enable the client certificate validation only in one of the following situations:

- Your network has implemented a complete PKI (Public Key Infrastructure) system, including a CA server, client software, and the appropriate operational procedures. Client hardware, tokens, and smartcards are optional.
- The CA's public certificate is installed in the RealPresence Capture Server system so that it trusts the CA.
- All authorized users' systems, including yours, have a client certificate signed by the CA that authenticates them to the RealPresence Capture Server system.

To enable the client certificate validation:

1. Go to **Configuration > Certificate Management**.
2. Tick **Enable web client certificate validation**.
3. Click **OK**. The system restarts to apply your changes.

Use OCSP to Obtain Revocation Status

You can enable OCSP (Online Certificate Status Protocol) to obtain the revocation status of a certificate presented to the system.

If the certificate includes an AIA extension, the system has the information needed to configure OCSP for obtaining revocation status.

To configure OCSP:

1. Go to **Configuration > Certificate Management**.
2. Select **Enable** OCSP.
3. Click **OK**. The system restarts to apply your changes.

You need to check **Enable web client certificate validation** firstly for OCSP to take effect.

Use HTTP protocol to access website

In addition to HTTPS, you can now access the website using HTTP protocol.

To enable HTTP protocol for server website:

1. Go to **Configuration > Certificate Management**.
2. Select **Enable HTTP protocol for Server Website** check box under **Client Certificate.**
3. Click **OK**.

Configure QoS

QoS (Quality of Service) is very important in transmission of high-bandwidth audio and video data. You can use QoS to test and guarantee the following settings:

- Average packet delay
- Delay variation (jitter)
- Error rate

To specify QoS parameters:

1. Go to **Configuration > QoS**.
2. Configure the following settings:

QoS parameters

Parameter	Description
Enable QoS for Signaling and Media	Enable configuration of the QoS settings. if not selected, the system uses the default QoS settings.
Type	**DiffServ** and **Precedence** are two methods for encoding packet priority. The priority set here for audio and video packets should match the priority set in the network routers. • **Differv**: Select when the network router uses **Differv** for priority encoding. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-63. **Note:** If you select **DiffServ** but your router does not support this standard, IP packets queue on the same communication links with data packets. This non-prioritized queueing greatly increases the latency and jitters in their delivery and can negatively impact performance. • **Precedence**: Select this option when the network router uses **Precedence** for priority encoding, or when you are not sure which method is used by the router. **Precedence** should be matched with **None** in the **ToS** field. The value range is 0-5. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-5. **Note: Precedence** is the default mode as it is capable of providing priority services to all types of routers and is currently the most common mechanism.
Audio / Video	Specify the priority for audio and video IP packets. The recommended priority is 4 for audio and video to ensure that the packet delay for both is the same, that audio and video packets are synchronized, and to ensure lip and audio synchronization (lip sync).
Control	Specify the priority for controlling packets.
ToS	Select the ToS (Type of Service) that defines optimization tagging for routing the conference audio and video packets. • **Delay:** The recommended default for video conferencing: prioritized audio and video packets tagged with this definition are delivered with minimal delay. • **None:** No optimization definition is applied. This is a compatibility mode in which routing is based on **Precedence** priority settings only. Select **None** if you do not know which standard your router supports.

3 Click **OK**. The server restarts to apply your changes.

QoS settings applies to SIP and H.323 calls only, it does not apply to streaming.

Configure SNMP

Your system provides a standard SNMP (Simple Network Management Protocol) interface which supports SNMP version 1, version 2, and version 3 queries with confidentiality, authentication, and integrity functions

conforming to SNMP MIB. The interface uses a common MIB, making it interoperable with Polycom CMA, DMA, and RMX systems.

- Available configurable options vary with the SNMP agent version and security level selected.
- RealPresence Capture Server does not support SNMP trap.

To configure SNMP settings:

1. Click **Configuration > SNMP**.
2. Select **Enable SNMP**.

   SNMP is disabled by default.
3. Configure the following agent parameters:

SNMP Parameters

Parameter	Description
Retrieve MIB Files	Retrieve MIB file to your computer.
Agent Name	Specify the name of this RealPresence Capture Server agent.
Contact Country	Specify the contact country for this RealPresence Capture Server.
Contact Person	Specify a contact person for this RealPresence Capture Server.
SNMP Agent Version	Specify the SNMP Agent version.

4. Configure the following security settings:

Security Settings

Parameter	Description
Accepted Host Community Name	Specify the community name that the host belongs to.
User Name	Specify the user name that will be used to log in over the **Authentication Protocol**.
Authentication Protocol	Specify the type of encryption to use when connecting with this user: • **MD5**: Message Digest 5 • **SHA**: Secure Hash Algorithm
Authentication Password	Specify the password that will be used to log in over the **Authentication Protocol**. **Note**: A valid password contains 8-64 characters, and not include these characters: &,',",<,>,%,|,+,=

Privacy Protocol	Specify the privacy protocol that you want to use: • **DES**: Data Encryption Standard • **AES**: Advanced Encryption Standard
Privacy Password	Specify the password that will be used to log in over the privacy protocol. **Note**: A valid password contains 8-64 characters, and not include these characters: &,',",<,>,%,|,+,=

Notice about Using Polycom SNMP MIB Files

Besides standard SNMP MIB files, RealPresence Capture Server also provides two proprietary MIB files:

- POLYCOM-BASE-MIB.mib
- POLYCOM-REAL-PRESENCE-MONITORING-MIB.mib

To use these Polycom MIB files, please first import the file POLYCOM-BASE-MIB.mib, then POLYCOM-REAL-PRESENCE-MONITORING-MIB.mib. Otherwise, the Polycom MIB files cannot be correctly compiled.

All RealPresence Capture Server MIB files can be downloaded from the Admin Interface **Configuration > SNMP > Retrieve MIB Files**.

Diagnostics

You can use Ping to verify that the RealPresence Capture Server system can communicate with another node in the network.

To run Ping on the RealPresence Capture Server system:

1. Go to **Configuration > Diagnostics**.
2. Enter an **IP Address or Host Name** and click **Ping**.
3. You will see the ping response shown in the ping result.

Active Directory

The Polycom RealPresence Capture Server system supports integration with a single Active Directory server.

After the integration, users in the Active Directory domain can access the Admin Portal or User Portal of the Polycom RealPresence Capture Server system directly as ordinary users without needing to be registered directly in the Capture Server system user database.

To configure an Active Directory server

1. Go to **Configuration > Active Directory**.
2. Configure the following settings:

Parameter	Description
Enable Active Directory	Specify whether to enable Active Directory functionality for this system.
Active Directory Address	Set the IP address or domain name of the Active Directory server to be integrated. Note: If you set a domain name, make sure you have already set a DNS server address that can resolve this domain name in **Configuration > IP Settings**.
Active Directory Port	Specify the port number for the Active Directory, the default value is 636.
Active Directory User	Set the user name that will be used by the Polycom Capture Server system to access resources on the Active Directory server.
Active Directory Password	Set the user password that will be used by the Polycom Capture Server system to access resources on the Active Directory server.
Active Directory Base DN	Can be used to restrict the Capture Server system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain). Leave the default setting, All Domains, initially.
Enable SSL Connection	Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the AD server.
Synchronize AD Time Point	Specify when to synchronize AD data on a daily basis.
Test	Test whether the Active Directory server is reachable.

3 Click **OK**

When the RealPresence Capture Server system is connected to the Active Directory server, **Active Directory Status** on the page displays **Connected**.

If the system is configured with an Active Directory server, users defined on the Active Directory can log in to the Polycom RealPresence Capture Server system as ordinary users. When logging in to the Polycom RealPresence Capture Server system's Admin Portal using an existing domain user, the user gets only ordinary user permissions.

Password Settings

Go to **Configuration > Password Settings** you can manage your password, learn how to change the security policies that control what kind of password you use and how often you have to change it.

Security Policy Parameters

Parameter	Description

Password Management	Password Expired Warning Period	Specify how far in advance the system displays a warning that the password will soon expire, if a maximum password age is set. Default: 10 (days)
	Maximum Password Age	Specify the maximum number of days that can pass before the password must be changed. Default: 90 (days)
	Minimum Password Age	Specify the minimum number of days that must pass before the password can be changed. Default: 0
	Reuse Number of Password	Specify the number of most recent passwords that cannot be reused. For example, if set to 2, the last two passwords cannot be reused. Default: 0
Password Complexity	Allow to contain or reverse User ID	Specify whether to allow a valid password to contain the same characters, in the same order or reversed, as the user name.
	Minimum Password Length	Specify the minimum number of characters required for a valid password. Default: 1 (day)
	Minimum Password Changed Characters	Specify the number of characters that must be different or in a different position in a new password. If this is set to 3, “123abc” can change to “345cde” but not to “234bcd”. Default: 0
	Maximum Consecutive Repeated Characters	Specify the maximum number of consecutive repeated characters in a valid password. If this is set to 3, “aaa123” is a valid password but “aaaa123” is not. Default: 0
	Minimum Upper Case	Specify the minimum number of uppercase characters required for a valid password. Default: 0
	Minimum Lower Case	Specify the minimum number of lowercase characters required for a valid password. Default: 0
	Minimum Numeric Characters	Specify the minimum number of numbers required for a valid password. Default: 0
	Minimum Special Characters	Specify the minimum number of special characters required for a valid password. Supported characters include the characters displayed in the Special Characters Set field. Default: 0

The value 0 indicates no limitation to this option.

UI Customization

You can personalize the system appearance, for example, set the IVR information and set an e-mail address for your RealPresence Capture Server system

Customize IVR Information

The RealPresence Capture Server system provides IVR (Interactive Voice Response) service. After the call to capture server is connected, the IVR will provide guide information to the user on the event happening at the capture server.

To customize the IVR information:

1. Go to **Configuration > Customization.**
2. Select the IVR information to be played and corresponding language option.
3. Click **Upload**.

   The audio file to be uploaded must be in PCM format, and the sampling frequency must be 16KHz, 16bit, and mono.
4. Click **Add**, select the audio file and click **Open**.
5. Click **OK**.

Default IVR Messages

Message Type	Message Text	When Played
Welcome	Welcome to conference record playback service.	When join the recording service where **Start Recording Immediately** is disabled.
Recording Started	Conference recording has started.	The conference recording has started.
Recording Stopped	The conference recording has ended.	The conference recording has ended.
Recording Paused	The conference recording is now paused.	The conference recording is paused.
Recording Resumed	The conference recording is now resumed.	The conference recording is resumed.
Disk Warning	You have exceeded your allocated disk space.	When there is not enough disk space to make recordings.
Call will be ended soon	The conference recording will end in another 10 minutes.	The conference recording is about to end in 10 minutes.
Playback Ended	Your playback has ended.	When the playback is ended.
Playback not allowed	You are not allowed to play back this archive.	You do not have permission to play back the archive after three failed attempts to input personal code.
Playback not processed	Sorry, your playback request can not be processed.	When play back an invalid archive.
Playback paused	Your playback is paused.	When the playback is paused.
Playback stopped	Your playback is stopped.	When the playback is stopped
Playback session timeout	Your session has timed out, your call will hang up.	When play back an archive with enabled PIN code protection, if you do not input PIN code within 15 seconds or if the playback is paused for five minutes.
Input personal code	Please enter your personal code and then press the pound key.	When play back an archive under PIN code protection.
Invalid personal code	Invalid personal code, please try again.	When play back an archive with invalid PIN code.

Customizing UI Logo

You can customize the logo displayed on both Admin Portal and User Portal.

To customize the Logo picture of the web Management interface:

1. Go to **Configuration > Customization**.
2. In the **Logo** area, click **Change Logo > Add** to select the picture to be uploaded.
3. The uploaded pictures must be in the *.png format, with 201 * 54 pixels.
4. Click **Open > Upload**.
5. Click **OK**.

Setup E-mail

You can set an e-mail address for your RealPresence Capture Server system. This is filled to “From” address in the e-mail the system sent out.

To set an e-mail address for the RealPresence Capture Server system:

1. Go to **Configuration > Customization**.
2. Configure the following settings:
   - **Admin Email Settings**
     - **Sender Email:** This is filled to “From” address in the email the system sent out.
     - **Frequency:** Select the period for automatic e-mail notification.
     - **Receiver Email:** The email is sent when there is administrative event occurs, like disk warning, alert, etc.
   - **Service Email Settings**
     - **Enable Emaill Notifications:** When enabled, you will receive e-mail notification when live streaming starts or archive is ready for VoD.

Portal Settings

- When using Polycom RealPresence Media Manager or other external portal to allow users to access live and on-demand streams, it is a best practice to redirect visitors from the Capture Server's User Portal to the Media Manager (or 3rd party portal) home page.
- You can also manage session idle timeout and maximum number of login for both Admin and User Portal.
- You can select to show both internal and external live streaming URL.

Portal Setting Configuration

Parameter		Description
Redirect Settings	Redirect users attempting to connect to User Portal (https://Capture_Server/portal) to the following URL:	Enter a URL for visitors to redirect from Capture Server's User Portal to the Media Manager (or 3rd party portal) home page.
	Test	Test whether the URL works.
	Disable view permission of user portal for guest user	This is enabled by default and as a result, guest users on User Portal do not have view permission.
Session Management	Admin Portal	• **Session Idle Timeout:** specifies the number of minutes an Admin Portal session can be idle before the server cancels the session. The default value is 30. • **Session Maximum Number Per Application:** The maximum number of Admin Portal login. The default value is 200
	User Portal	• **Session Idle Timeout:** specifies the number of minutes a User Portal session can be idle before the server cancels the session. The default value is 30. • **Session Maximum Number Per Application:** The maximum number of User Portal login (including anonymous login). The default value is 3000.
Streaming URL Settings	Show both internal and external live streaming URL	When selected, portal will show both external media server's live stream URL and Capture Server's native stream URL. By default this option is unchecked and only external media server's live stream URL is shown.

Record and Playback

Configure Templates

A template is used to define a set of basic recording parameters, such as call rate of recording, video quality, whether to live stream and streaming rate. All Virtual Recording Rooms (VRR) are created based on templates. Changing parameters of a template may change the corresponding recording policies of the VRR using that template.

Configure Recording Templates

In this section you'll learn how to configure recording templates, including how to view, define, edit or delete a recording template.

To view a recording template:

» Go to **Template > Recording Templates**.

To define a recording template:

1 Go to **Template > Recording Templates**.
2 Click **Add**.
3 Configure the following settings:

Recording Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Enable Live Streaming	Enable live streaming for the calls that use this template.
Disable Recording	This setting is available when **Enable Live Streaming** is selected. When this is selected, the call will be live streamed only, without recording.
Enable Multicast	Specify whether to enable multicast for the recording template. If **Auto Multicast for Live Streaming** isn't enabled in system configuration, users can enable multicast for this template.
Multicast TTL (available after multicast is enabled)	Choose from the drop-down list. The default TTL value is **Auto -- Use System Setting**. Note: The template value set here will override the system value.

Enable PIN	Specify whether to enable PIN code protection for the archive. If a PIN code is set, you must enter the correct PIN code to play the live streams or archives created using this VRR. After this option is selected, you must enter a PIN code consisting of 1-16 digits in **PIN Code**.
Call	
Audio Only	Select this check box to define the recording for the call with this template has only audio capability, no matter the call rate negotiated.
Max Call Rate	Specify the maximum bandwidth that can be used by an endpoint or MCU to connect to the RealPresence Capture Server system for recording and live streaming.
Max Resolution	Specify the maximum resolution of people video that can be used to connect to the RealPresence Capture Server system for recording and live streaming.
Enable LPR	Once this function is selected, in case of packet loss during network transmission, it can effectively improve the decreased video quality caused by packet loss.
Indication Tone	Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second. This is enabled by default.
Media Encryption Type	If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled and SIP connections: • **Required For All Calls:** Enable the AES encryption for all H.323 and SIP calls, including video and audio only calls. This option requires the device to connect the system with AES enabled, otherwise, the connection cannot be set up. • **When Available:** Both encrypted and non-encrypted undefined participants can connect to the same conferences, where encryption is the preferred setting. • **Off:** Disable the AES encryption and SIP connections. Note: The Media Encryption Type available here is consistent with that set under Set Recording Parameters. The encryption change is applied to new calls only and does not impact the archive.
Max Call Length	Specifies the maximum call length for recording or live streaming calls. The default option is **Auto** (When selected, the max call length setting will be the same as configured under **Configuration > Call Settings**). Note: The template value set here will override the system value set under **Configuration > Call Settings** on Admin Portal.
Conference Layout (RMX 8.4 or higher)	Specify the people layout received and recorded from MCU. The **1x1** and **1x2** layout may give focus on the speaker of the conference in the recording. • **Auto:** Automatic layout according to conference setting at RMX side to recording server. • **1x1:** Single view to recording server. • **1x2:** Dual view to recording server.
Archiving	

Start Recording Immediately	If this option is selected, the system immediately starts recording with this recording template. If deselected, you may need to manually start recording through the Admin Portal or the TV UI.
Archive Name Prefix	Specify the prefix of the output media archive name.
Live Streaming (MP4)	
Enable H.264 High Profile for Live Streaming	Select this check box to enable the use of H.264 High Profile in Video Switching conferences.
Primary Streaming Rate (Kbps)	The default value is 1024 kbps. Once the streaming rate is set, you can define a name for this streaming.
Secondary Streaming Rate (Kbps)	The default value is **Off**. After a streaming rate is set here, you can define a name for this streaming.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video at the right side. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video at the left side. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent.
Live Streaming (WMV)	
Primary Streaming Rate (Kbps)	The default value is **Off**. Once the streaming rate is set, you can define a name for this streaming.

Secondary Streaming Rate (Kbps)	The default value is **Off**. Once the streaming rate is set, you can define a name for this streaming.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** The stream supports dual windows on Windows Media Player, one for people video, the other for content video, black screen displays when content is absent.

4 Click **OK**.

You can click **Save As** to clone a new template with the same settings.

To edit or delete a recording template:

1 Go to **Template > Recording Templates.**
2 Click the recording template you want to change.
3 Click **Edit** or **Delete**.

Max Call Length

Maximum call length is used to restrict the call length for recording and streaming calls due to the following reasons:

- When record a meeting, the recording call may be endless (to RMX for example) and thus flood the disk for unused data.
- A recording longer than 8 hours is difficult to be offline-transcoded.
- An endless streaming only session will cost transcoding resource occupancy.

To set max call length for recording and streaming calls

1 Go to **Template > Recording Templates**.
2 Select the recording template you want to change.

3 Click **Edit**.

4 Choose a value from the **Max Call Length** drop-down list.

- The max call length is a guard timer used to automatically stop recording and disconnect to the recording client when timer times out. This is helpful to avoid flooding the disk if recording server fails to end the call after the recording event.
- For a recording call (with or without live streaming), the default setting is 2 hours, range is 1-8 hours; for live streaming only calls, default setting is 8 hours and there is no limitation to max range
- When a call is approaching the max call length, an IVR message will be sent to user as a reminder.

To set max call length for streaming only calls:

1 Go to **Template > Recording Templates.**

2 Click the recording template you want to change.

3 Click **Edit**.

4 Select **Disable Recording**.

5 Clear **Auto** underneath **Max call Length**.

6 Enter your desired value.

Note: Input positive numbers and the value 0 indicates no limitation to this option.

Configure Transcoding Templates

In this section you'll learn how to configure transcoding templates, including how to view, define, edit or delete a transcoding template, you can also learn how to replicate transcoding templates for external media servers.

To define a transcoding template:

1 Go to **Template > Transcoding Templates**.

2 Click **Add**.

3 Configure the following settings:

Transcoding Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Media Type	Specify the output media file format.
Bit Rate	Specify the output media file bitrate.
Video Type	The video protocol used by the archive.
Frame Rate	Specify the media frame rate.
Max Resolution	Specify the maximum transcoding resolution.

Aspect Ratio	Specify the aspect ratio of the output media file.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (people 75%; content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with large content (people 25%; content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** The stream supports dual windows on Windows Media Player, one for people video, the other for content video, black screen displays when content is absent. Note: This option is only available when you set **Media Type** as **WMV**.
Enable VOD Timecode watermarking	Specify whether to enable Timecode (GMT) Watermarking functionality for VoD.
Transfer to Media Server	For ISM format, you can transfer media files to IIS Media Server. For MP4 format, transfer media files to WOWZA server. For WMV format, transfer to Windows Media Server. For external media server configuration details, refer to Appendix B.
Snapshot Enable	Specify whether to generate snapshots for transcoded media files.
Remove Duplicate Thumbnail	Delete the duplicate snapshots resulted during thumbnail generation process.
Enable auto snapshot during entire call	When enabled, snapshots could be generated automatically throughout the entire call.
Start Time	Select the start time for the automatic snapshot.
End Time	Select the end time for the automatic snapshot.
Interval	Set the snapshot interval, measured in second.

4 Click **OK**.

You can click **Save As** to clone a new template with the same settings.

You can find some preconfigured templates for iOS and Android as follows:

Preconfigured Templates for iOS

Template Name	Resolution	Frame Rate	Bitrate	Aspect Ratio	Device	Profile
Iphone_M_2	640*480	30	1296	4:3	iPhone4 & above	Baseline
Iphone_S_2	480*360	15	464	4:3	iPhone4 & above	Baseline
Ipad_L	1024*768	30	1M	16:9	iPad 2, iPad mini	Baseline
Iphone_M_1	640*360	30	664	16:9	iPhone4 & above	Baseline
Ipad_H	1920*1080	30	1.7M	16:9	New iPad, iPad Retina Display	High Profile
Iphone_S_1	480*270	15	464	16:9	iPhone4 & above	Baseline

Preconfigured Templates for Android

Template Name	Resolution	Frame Rate	Bitrate (Kbps)	Profile
SD_H	480*360	30	500	Baseline
SD_L	176*144	12	56	Baseline
HD	1280*720	30	2M	Baseline

To view a transcoding template:

- » Go to **Template > Transcoding Templates**.

To configure a transcoding template for IIS media server:

1. Go to **Template > Transcoding Templates**.
2. Click **Add.**
3. Select **ISM** for **Media Type**.
4. Select the IIS media server you configured in **Transfer to Media Server** field.

To configure a transcoding template for WOWZA media server:

1. Go to **Template > Transcoding Templates**.
2. Click **Add.**
3. Select **MP4** for **Media Type**.
4. Select the WOWZA media server you configured in **Transfer to Media Server** field.

To edit or delete a transcoding template:

1. Go to **Template > Transcoding Templates.**
2. Click the transcoding template you want to change.
3. Click **Edit** or **Delete**.

Configure VRRs

A VRR defines recording parameters. You can create a VRR basing on recording templates. A VRR is identified by digits, and you can directly start recording using a specified VRR by adding the VRR number to the dial-in number.

A default VRR, named *DefaultVRR*, is built in the system. When an endpoint or MCU tries to connect by dialing the RealPresence Capture Server without VRR number specified, default VRR parameters are used. You can modify the default VRR but cannot delete it.

To define a VRR:

1. Go to **Template > VRRs**.
2. Click **Add**.
3. Configure the following settings (* indicates mandatory parameters).

VRR Parameters

Parameter	Description
VRR Name	Specify a unique name to identify the VRR. You can also use the default name generated by the system.
VRR Number	Specify a number to identify the VRR. You can directly dial the VRR to record by adding the VRR number when dialing the RealPresence Capture Server system. The number you entered must be unique and comprised of 4-8 digits. You can also use the number automatically generated by the system. Note: The initial digit of the VRR number cannot be zero.
Description	If necessary, you can enter additional VRR information, such as the owner and usage, in order to improve identification and classification management when there are many VRRs.
Recording Template	Specify the recording template. The template defines the basic recording link parameters.

Transcoding Template	After recording is done, the system will do offline transcoding according to transcoding templates configured here. Multiple offline transcoding outputs are allowed. Note: Only qualified transcoding template will apply. If the template parameters is higher than recorded raw parameters, then the template will be ignored. For example, if recording raw resolution (e.g. 4CIF) is less than transcoding template (e.g. 720p), then this transcoding template will be ignored.
Live Streaming Server	You can check configured live streaming server information including publish point template, stream alias, and streaming list.
Email Address (separated by ‘,’)	Once the live streaming is started or the VRR recorded video has completed its format conversion and is ready for viewing, the system sends an e-mail message to the address set here.

4 Click **OK**.

You can click **Save As** to clone a VRR with the same settings.

To add publishing points for external media servers:

1 Go to **Template > VRRs.**

2 Select a VRR and click **Edit**.

3 Click Add **,** select a live streaming server you configured**.**

4 Enter values in the **Publish Point Template** field.

5 Fill in an alias for this stream.

6 Select a live streaming bitrate.

For external or AKAMAI media server configuration details, refer to Appendix B.

7 Click Save .

Always click **Save** before clicking **OK**; otherwise the entered data will be lost.

8 Click **OK**.

To edit or delete a VRR:

1 Go to **Template > VRRs**.

2 Click the VRR entry you want to edit or delete.

3 Click **Edit** or **Delete**.

Start a Recording

You can start recording in RealPresence Capture Server using one of the following methods:

- Call from RealPresence Capture Server to an interoperable endpoint from Admin Portal.
- Call from RealPresence Capture Server to an interoperable endpoint from User Portal
- Call RealPresence Capture Server from an interoperable endpoint.
- Start a recording from Polycom RMX system via recording link.

- Schedule a meeting on RealPresence Media Manager and connect the RealPresence Capture Server to an endpoint.

To start a recording from the Admin Portal:

1. Access Capture Server admin portal by its IP address or host domain name from a compatible browser.
2. Enter the user name and password to log in to the system.
3. Go to **Home.** In the **Signaling Connection** area, click **Dial out to record**.
4. Configure the following settings:

Dial Out Parameters

Parameter	Description
Address	Specify the calling address. The system supports entering the calling address with an extended service number in the address box. If you call a H.323 system, you can dial out to endpoints by entering the numbers in the following formats: • [far end E.164 prefix] - Use when every system has registered to a gatekeeper. For example, if a far end system E.164 prefix is 9988. • [Far End H.323 ID]- Use when every system has registered to a gatekeeper. For example, if a far end system H.323 ID is CS9988. • [Far End IP Address]- Use when a system has not been registered to a gatekeeper. For example, if a far end system IP address is 172.22.33.44.
Signal	Set the H.323 or SIP network type for the system to place a call. Your choice depends on the call type used by the peer device.
VRR Name	Click **Select** to select a virtual recording room (VRR). You can use the built-in default VRR, or one you have created. A VRR defines recording policies. For more information, refer to Configure VRRs.
Event Name	Specify a unique name for this event.
Max Call Rate (Kbps)	Display the maximum call rate specified in VRR

5. Click **OK**.

Unlike administrators, normal users can only view and manage calls started by themselves.

Dial in from Endpoint

You can start recording by dialing RealPresence Capture Server or dial in to a VRR directly to start recording.

To start recording by dialing RealPresence Capture Server:

» Enter the E.164 prefix or H.323 ID or SIP URL of RealPresence Capture Server on the user interface of an interoperable endpoint, for example, from remote control of HDX or Group Series.

If your system or endpoint is not registered to the gatekeeper or to a SIP server, call the system IP address instead.

You can also dial in to a VRR directly to start recording by dialing one of the following:

For H.323 calls

- `[RealPresence Capture Server IP]##[VRR number]`

  For example, if the `RealPresence Capture Server IP is 11.12.13.14`, and the VRR number is `4096`, dial *`11.12.13.14##4096`*.

- `[RealPresence Capture Server E.164 prefix][VRR number]`

  For example, if the RealPresence Capture Server E.164 prefix number is 8888, and the VRR number is 4096, dial *`88884096`*.

For SIP calls

- `[VRR number]@[RealPresence Capture Server IP]`

  For example, if the `RealPresence Capture Server IP is 11.12.13.14`, and the VRR number is `4096`, dial *`4096@11.12.13.14`*.

- `[SIP peer prefix][VRR number]`

  If the system has been registered to a SIP server, the SIP server should configure CaptureServer as a SIP peer. For example, if the SIP peer prefix of the Polycom RealPresence Capture Server system is 8888 and the VRR number is 4096, the dial string should be 88884096.

Record from RMX via Recording Link

Capture Server can automatically record, or automatic record and stream, when RealPresence Collaboration Server (RMX Series) is configured with a Capture Server Recording Link has enable in RMX Conference Profile. Refer to the Collaboration Server (RMX Series) Getting Started Guide and Administrator's Guide.

Change Conference Layout for RMX Hosted Calls

Once the Capture Server Recording Link is enabled on RealPresence Collaboration Server system (version 8.4 or higher), a user dials into a conference hosted on RealPresence Collaboration Server, the layout can be changed once Capture Server is connected when configured with SIP calls only.

To set conference layout type in a recording template

1. Go to **Template > Recording Templates**.
2. Select a recording template you want to edit.
3. Click **Edit**.
4. Choose from the **Conference Layout** drop-down list:
   -

Auto: Automatic layout according to conference setting at RMX side to recording server
   -
1x1: Single view to recording server.

- **1x2:** Dual view to recording server.

To change conference layout type for an ongoing call

1. On Capture Server Admin Portal, go to **Signaling Connection** and click
2. Choose from the following layouts:
   - **Auto:** Automatic layout according to conference setting at RMX side to recording server.
   - **1x1:** Single view to recording server.
   - **1x2:** Dual view to recording server.

When an endpoint or MCU tries to connect by directly dialing the IP address or E.164 prefix of the RealPresence Capture Server system, the default VRR parameters are used to record. You can directly start recording using recording parameters defined in a VRR by adding the VRR number to the dial-in number.

If the RealPresence Capture Server system is configured in connection with a Polycom RMX series system through the recording link, you can specify the VRR to be used by adding the VRR number in the **Recording Link** field on the Polycom RMX system. For more information, refer to the Polycom RMX system Administrator's Guide.

For prefix+VRR format, you need to add SIP Peer to Polycom DMA server, for details, refer to the Polycom DMA server's Administrator's Guide.

With the newly added Annex-O support, you can start recording by dialing one of the following:

• For incoming calls to Capture Server, the dial-in number is [VRR number]@[RealPresence Capture Server IP address].

• If you call from RealPresence Capture Server to an interoperable endpoint such as Polycom HDX Series system, the dial-out number is [RealPresence Capture Server E.164 suffix]@[HDX IP Address] or [RealPresence Capture Server H.323 ID]@[HDX IP Address]

• If you call from RealPresence Capture Server to a MCU, the dial-out number is [Conference ID]@[RMX IP Address]

Point-to-point Recording

Point-to-point recording allows a user to dial out to two endpoints from the Capture Server Admin Portal or User Portal, and record the two sites into same recording file.

To start point-to-point recording from Admin Portal

1. In the address line, enter the system's IP address in this format: https://<system IP address>/admin.
2. Enter the user name and password to log in to the system.
3. Go to **Home or Call.** In the **Signaling Connection** area, click **2 Sites Recording**.
4. Enter the addresses of the two H.323 endpoint participants.
5. Click **OK**.

- For now it is only available in H.323 point-to-point calls.
- For point-to-point recording from User Portal, refer to To start point-to-point recording from User Portal

Video Call Playback

This section introduces how to play back video files for both dial-in and dial-out calls.

Video Call Play Back when Dialing in from Endpoint

You can play back recorded media archives stored in RealPresence Capture Server using Quick Code. A quick code is generated automatically for every archive after the system completes a recording.

To view the quick code of an archive from Admin Portal

1. Go to **Media > Archives**.
2. The quick code is displayed in the **Quick Code** column.

If you need to view the quick code of an archive from User Portal, log in to the User Portal firstly, the quick code is displayed beneath the archive names.

To edit the quick code of an archive:

1. Go to **Media > Archives**.
2. Select an archive.
3. Click **Edit**.
4. Edit the quick code in **Quick Code** text filed.
5. Click **OK**.

To play back archives using the quick code:

» Dial using one of the following formats:

A quick code consists of 7 digits that start with the number 0. If the archive has multiple episodes, you can append the two-digit episode index to the seven-digit quick code in your dial string.

➢ **H.323:**

♦ If the system has been registered to a gatekeeper, dial [Capture Server E.164 prefix][Quick Code]

For example, if the E.164 prefix of the Polycom RealPresence Capture Server system is 1234 and the quick code of the file to be played back is 0123456, dial 12340123456

- If the system has not been registered to a gatekeeper, dial [RSS IP address]##[Quick Code]

  For example, if the IP address of the Polycom RealPresence Capture Server system is 10.1.2.3 and the quick code of the file to be played back is 0123456, dial 10.1.2.3##0123456

➢ **SIP:**

- If the system has been registered to a SIP server, the SIP server should configure CaptureServer as a SIP peer, dial [SIP Peer Prefix][Quick code].

  For example, if the SIP peer prefix of the Polycom RealPresence Capture Server system is 1234 and the quick code of the file to be played back is 0123456, dial 12340123456.

- If the system has not been registered to a SIP server, dial [Quick Code]@[RSS IP address]

  For example, if the IP address of the Polycom RealPresence Capture Server system is 10.1.2.3 and the quick code of the file to be played back is 0123456, dial 0123456@10.1.2.3

  If you want to play back the second episode of the archive, you can replace the quick code in above dial string by appending episode index, such as replace 0123456@10.1.2.3 with 012345602@10.1.2.3.

- If no press on your part, it will begin playing the next episode automatically 30 seconds after the end of the previous one.
- Once the archive playback is completed, Capture Server will drop from the multipoint call within five minutes if no command is given.
- Capture Server will terminate the call five minutes after the playback is paused.
- If the capacity supports 40 recordings only, the Quick Code playback function is not supported.

Video Call Playback when Dialing out from Capture Server

RMX Playback (RMX 8.5 or higher)

If the Capture Server system dials into a conference hosted on RealPresence Collaboration Server, the layout can be changed once Capture Server is connected when configured with SIP calls only.

To start a playback call:

1. On Capture Server Admin Portal, go to **Media > Archives**.
2. Select an archive and click **Playback**.
3. Fill in the IP address.
4. Choose a signaling protocol.
5. Choose from the following layouts:
   - ➢ **Auto:** Automatic layout according to conference setting at RMX side to recording server
   - ➢ **Lecture:** The playback video is viewed in full screen by all conference participants.
6. Choose an episode from the drop-down list.
7. Click **OK**.

- Once the archive playback is completed, Capture Server will drop from the multipoint call within five minutes if no command is given.
- Capture Server will terminate the call five minutes after the playback is paused.

When video call play back to RMX, the conference layout type can be changed. You can reuse the current overview.

To change conference layout type for an ongoing call

1. Go to **Signaling Connection** and click
2. Choose from the following layouts:
   - **Auto:** Automatic layout according to conference setting at RMX side to recording server.
   - **Lecture:** The lecturer is viewed in full screen by all conference participants, while the audience is “time-switched” in the speaker’s view.

It’s for SIP calls only.

Live Streaming

The RealPresence Capture Server system supports live streaming of video sources, such as live video conference or dual stream sent by endpoints or MCUs with a highest resolution of 1080p and a maximum bandwidth of 4M. Those live streaming videos are saved in the system.

Live streaming supports dual streaming rates; this allows you to choose the appropriate bandwidth to view video based on your network condition.

Multi-bitrate Live Streaming

If the recording template is configured, the Capture Server system could send a specific resolution live stream to low bandwidth sites and a higher quality resolution live stream to high bandwidth sites without creating separate video broadcasts.

To live stream meetings to an external server, follow these steps:

1. Configure the external media server on the RealPresence Capture Server system and enable live streaming.
2. Configure a recording template that enables live streaming.
3. Configure a VRR that enables external media server.
4. Record a meeting using the VRR that has the external media server enabled.

   Refer to the following instructions to configure the external media servers to work with the RealPresence Capture Server system.

To configure live streams in recording template

1. Go to **Template > Recording Templates**.
2. Select a recording template.
3. Click **Edit**.
4. Select **Enable Live Streaming**.
5. Go to **Live Streaming (MP4)** and select **Enable H.264 High Profile for Live Streaming**.
6. Set the **Primary Streaming Rate** and **Secondary Streaming Rate.**
7. Go to **Live Streaming (WMV)** and configure relevant settings.
8. Click **OK**.

For configuration details, refer to table "Recording Template"

Start Live Streaming

Procedure for starting a live streaming is the same as the one for starting recording. For more information, see Start a Recording

View Live Streaming Information

If live streaming is in progress on the system, the current live streaming list displays on the Live Streaming page. Go to **Media > Live Streaming** menu to enter the **Live Streaming** page.

The live streaming list displays live streaming summary, such as live streaming name, VRR number used, start time, live streaming detail and multicast detail.

View Live Streaming Video

When the system starts live streaming, you can view the video being live streamed in real time on the Live Streaming page.

To view live streaming in progress:

1. Go to **Media > Live Streaming**.
2. Select the live streaming content you want to view in the list, and then click ▶ in the **Live Streaming Details** area on the right side of the page. The system's User Portal opens to play the video.

   If the live streaming content uses two different bandwidths, two **Play** buttons with their bandwidths appear in this area, and you may choose the appropriate bandwidth to play based on your network condition.

You can also view live streaming links on **Home** and **Call.**

Configure External Media Servers

You can now stream live meetings and on demand meeting archives to leading 3rd party media servers, such as Wowza, IIS Media Service (Smooth Streaming only) and Windows Media Server.

Configure IIS or Wowza Media Server

You need to configure a Wowza or IIS media server and your RealPresence Capture Server to work with the server as well.

To configure IIS and WOWZA media servers:

1. Click **IIS** or **WOWZA** under **Server**.
2. Click **Add**.

3 Configure the following basic settings.

External Media Servers Parameters

Parameter	Description
Server Name	Specify the name of the external server.
Server Address	Specify the IP or DNS of the external server you selected.
Server Port	Specifies the port that the RealPresence Capture Server system uses to send the encoded MP4 live streams to the external server. Following are the default ports: • **IIS Media Server**: 80 • **Wowza Media Server**: 1935 **Note**: Valid port values range from 1-65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server.

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

Enable Live Streaming

Parameter	Description
Stream Protocol (for WOWZA only)	Choose between **RTSP Steaming** and **RTMP Streaming**.
Application Name	Specify the name of the external media server's application to be used for the live streaming. **Note**: Contact the administrator of the external media server for the naming rule of the application name.
User Name	Specify the user name to access the external media server.
Password	Specify the password to access the external media server.
Test	Test whether the live streaming configurations work.

Configure Windows Media Server

You need to configure a Windows media server and your RealPresence Capture Server to work with the server as well.

To configure Windows Media Server:

1 Click **Windows Media Server** under **Server**.

2 Click **Add**.

3 Configure the following basic settings.

External Media Servers Parameters

Parameter	Description
Server Name	Specify the name of the external server.
Server Address	Specify the IP or DNS of the external server you selected.
HTTP Port	The default value is 80.
RTSP Port	The default value is 554.

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

Enable Live Streaming

Parameter	Description
User Name	Specify the user name to access the external media server.
Password	Specify the password to access the external media server.
Test	Test whether the live streaming configurations work.

Configure AKAMAI CDN

You need to configure an AKAMAI media server and your RealPresence Capture Server to work with the server as well.

To configure AKAMAI Media Server:

1 Click **AKAMAI** under **Server**.

2 Click **Add**.

3 Configure the following basic settings.

External Media Servers Parameters

Parameter	Description
Configuration Name	The CONFIG NAME displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.
Stream Name	The STREAM NAME displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.
Stream Number	The STREAM ID displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.

Server Port	Specifies the port that the RealPresence Capture Server system uses to send the encoded MP4 live streams to the AMAKAI server. **Note**: Valid port values range from 1-65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the AKAMAI server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the AKAMAI server.
Entry Point	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
HDS Playback URL	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
HLS Playback URL	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
User Name	Specify your entry point user name to access the AKAMAI server.
Password	Specify your entry point password to access the AKAMAI server.

4 Click **OK**

This is a charged function and you need an account to log in to the AKAMAI configuration page to get the needed parameters.

To add publishing points for external media servers:

1 Go to **Template > VRRs.**
2 Select a VRR and click **Edit**.
3 Click Add **,** select a live streaming server you configured**.**
4 Enter values in the **Publish Point Template** field.
5 Fill in an alias for this stream.
6 Select a live streaming bitrate.
7 Click Save. Always click **Save** before clicking **OK**; otherwise the entered data will be lost.
8 Click **OK**.

Pre-link Event

Sometimes for significant events like webcast or CEO meetings you may need to send meeting logistics beforehand, this feature provides pre-link URL for recording, live streaming and multicast live streaming events.

To create a pre-link event:

1 Go to **Template > Events**.
2 Click **Add**.

3 Configure the following settings (* indicates mandatory parameters).

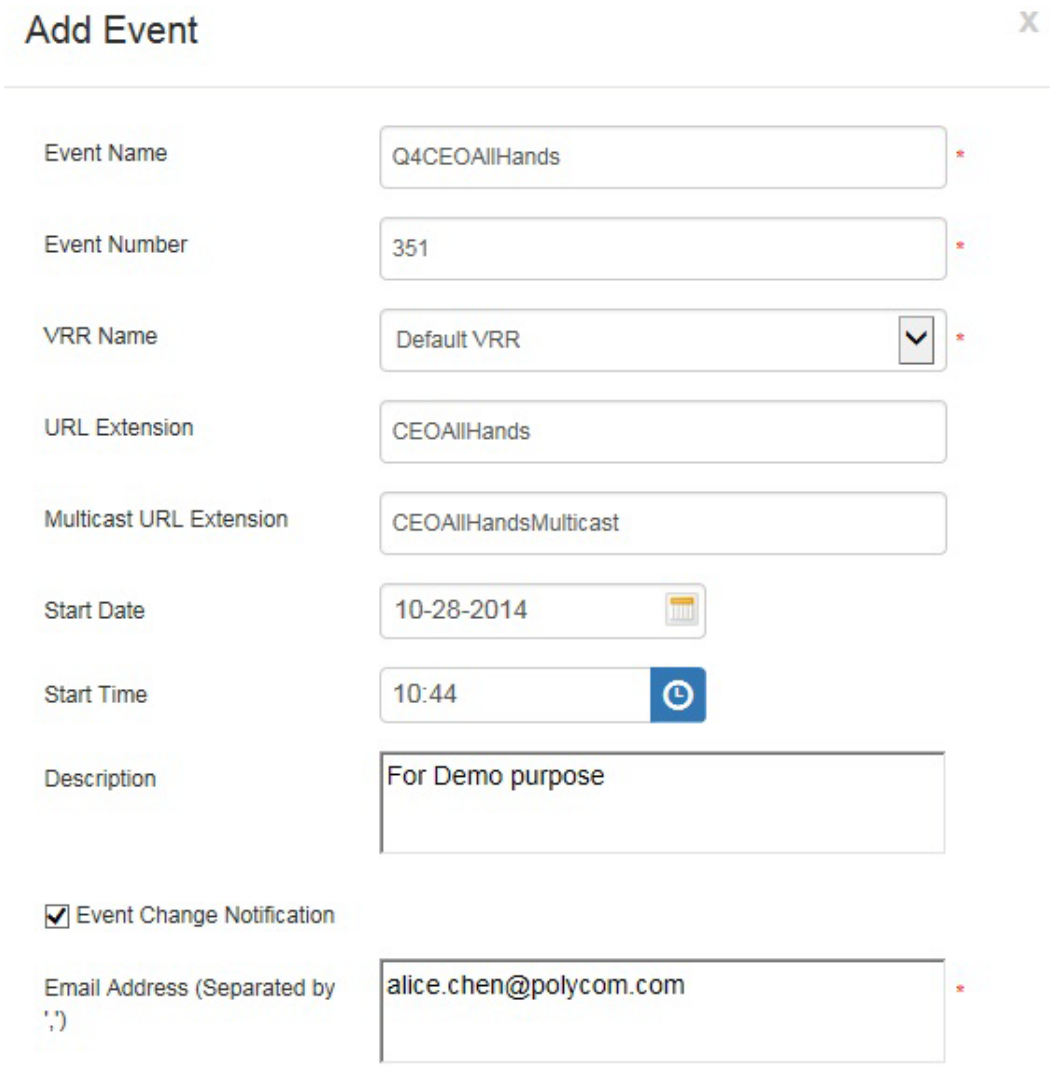
Pre-link Event Parameters

Parameter	Description
Event Name	Specify a unique name for this event. A valid event name contains lowercase characters (a–z), uppercase characters (A–Z), numbers (0–9), space or multibyte characters.
Event Number	Specify a number to identify the event, you can also use the number automatically generated by the system. Note: The valid number ranges from 300-399.
VRR Name	Choose a VRR from the drop-down list.
URL Extension	Extension of the streaming URL, this is available after live streaming is enabled for the recording template in the selected VRR. Note: You need to enable live streaming in recording template. Valid extension contains lowercase characters (a–z), uppercase characters (A–Z), and numbers (0–9).
Multicast URL Extension	Extension of the multicast URL, this is available after multicast is enabled for the recording template in the selected VRR. Note: You need to enable multicast in recording template. Valid extension contains lowercase characters (a–z), uppercase characters (A–Z), numbers (0–9).
Start Date	Which date the event will start. Note: The event cannot start automatically, the start date is for reference only.
Start Time	Which time the event will start. Note: The event cannot start automatically, the start time is for reference only.
Description	Specify additional related information.
Event Change Notification	When enabled, you receive e-mail notification once changes are made to the configured pre-link event settings.
Email Address (separated by ‘,’)	Once changes are made to the configured pre-link event settings, the system sends an e-mail message to the address set here. Separate several addresses with comma (,).

4 Click **OK**.

You need to fill out either **URL Extension** or **Multicast URL Extension**, otherwise the pre-link event is created but the pre-link URL will not be generated.

Add event example



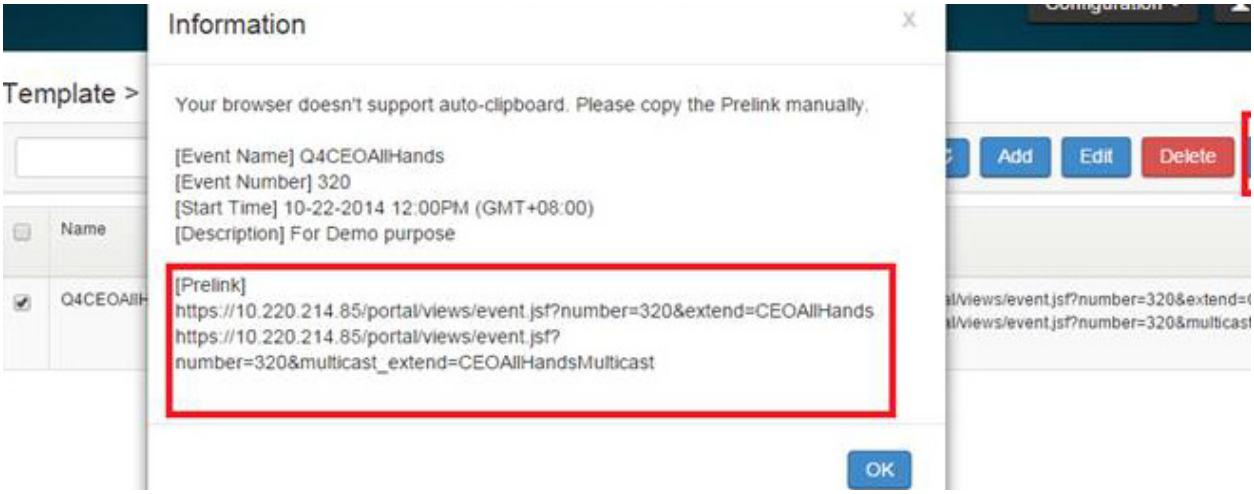
To edit a pre-link event:

1. Go to **Template > Events**.
2. Select the event you want to change.
3. Click **Edit**.

To obtain the pre-link URL extension:

1. Go to **Template > Events**.
2. Select an event from the list.
3. Click **Copy Prelink**.

Copy prelink information



4 Click **OK**.

- If you click the URL before or after the event, there will be a pop-up message **The stream is not available now**.
- When the event starts, the player will refresh the URL and display the stream.

To start the pre-link recording:

1 Go to **Home**.
2 In the **Signaling Connection** area, click **Dial out to record**.
3 Configure relevant settings. You need to select **Event Name** for the recording to start.
4 Click **OK**.

Media Management

You can archive your conferences and manage your archives.

Manage Archives

You can view all files recorded by the RealPresence Capture Server system in the **Media > Archives** page.

An administrator can view, play back, delete, download, or re-transcode these media files.

View Archive Details

On the **Media > Archives** page, administrators can view a summary of each archive.

Archive Details

Parameter	Description
ID	The ID for this archive.
Name	The name of the archive.
Duration	The duration of the archive.
Video Type	The video codec type used by the archive.
Audio Type	The audio codec type used by the archive.
Content Type	The content video type of the archive.
Key Words	The keywords for this archive.
Description	Additional user information.

Play Back and Download Archives

The RealPresence Capture Server system can transcode recorded videos into different formats, layouts and bit rates, including:

- **RAW**: RAW bit stream is automatically generated after the system completes the recording, also can be transcoded if transcoding template is configured.

  The RAW files are stored in a proprietary format. They are used as the source file to transcode other media formats. For detailed transcoding settings, refer to Configure Transcoding Templates.
- **MP4:** MP4 archives (Also known as H.264 streaming files) can be downloaded.

- **M4A:** M4A (audio only file) files can be downloaded to PCs, Macs, or to compatible digital media devices, but cannot be play backed from portals.
- **ISMV:** After the ISMV files are generated, they are uploaded to the IIS Media Server, and can be viewed from the User Portal.

  The ISMV files are generated only when the transcoding template is configured with IIS Media Server and the transcoding template is added in VRR.
- **WMV:** WMV files can be transcoded if transcoding template is configured. They can be downloaded to PCs or to compatible digital media devices.

To play back archives through the Admin Portal:

1. Go to **Media > Archives**.
2. Select the archive you want to play back.
3. Click and the User Portal opens to play the video.

   If the e-mail notification function has been enabled for the VRR that is used to record archives, the system sends you an e-mail notification automatically once all archives have been converted and are ready for web playback. For more information, see Configure VRRs.

To download one or several archives from Archives page:

1. Go to **Media > Archives**.
2. Select the archive you want to download.
3. Click **Download**.
4. Select one or several media types to download.
5. Click **OK**.

To download one or several media files from Media Files page:

1. Go to **Media > Archives**.
2. Select the archive you want to download.
3. Click **Media Files**.
4. Select one or several media files to download.
5. Click .

Manage Archives

You can edit or delete archives recorded by your own archives that you are authorized to modify.

To modify archive properties:

1. Go to **Media > Archives**.
2. Double-click the archive entry you want to modify.

3 If you are authorized to modify the archive, you can modify following parameters:

Archive Properties

Parameter	Description
Name	Specify the name of the archive. **Note:** Only letters, figures, _, space or multi-byte characters can be used for the file name, and the length is 4-20 characters.
Description	Specify additional related information.
Enable PIN	Specify whether to enable PIN code protection for the archive.
Key Words	Specify additional information related to the archive.
Quick Code	Generated automatically for every archive after the system completes a recording

4 If you want to change the list of users who can view or modify the archive, click the **Allowed Users/Groups** tab.

5 Choose an item (**Users/Groups/AD Groups**) from the drop-down list and click **Add**.

6 Click **OK**.

To delete one or several archive files:

1 Go to **Media > Archives**.

2 Select one or several archive files you want to delete.

3 Click **Delete**.

4 Click **OK** at the prompt message.

Dynamic Archiving

You can view all media files included in an archive, create new media output formats on the fly, stop ongoing media file creation, or delete existing media files. You can also restart transcoding after you stop the transcoding, or when there is transcoding error.

To add new media files:

1 Go to **Media > Archives**.

2 In the archives list, select an archive.

3 Click **Media Files**.

4 Select one media file.

5 Click **Add**.

6 Select one or several transcoding templates.

7 Click **Add,** and then click **Close.**

- Select a transcoding template with lower bit rate, resolution, and frame rate than that of the source file.
- Click **Media > Transcoding** to view the transcoding status.
- Once transcoding is done, find the transcoded files under **Media > Archives.**

To delete a media file:

1. Go to **Media > Archives**.
2. In the archives list, select an archive.
3. Click **Media Files**.
4. Click a media file to be deleted, and then click **Delete**.
5. Click **OK,** and then click **Close**.

Archives will be deleted permanently once you choose delete action on Admin Portal.

Transcoding Task Control

In this section you can learn how to view transcoding status, stop an ongoing transcoding, or restart a transcodong.

To view transcoding status:

1. Go to **Media > Transcoding.**
2. In the archives list, select an archive.
3. Click **Media Files**. Media files transcoding can have the following status:
   - Ready: The file can be played and downloaded.
   - Waiting: File waiting to be transcoded
   - Transcoding: File in transcoding.
   - Error: File with transcoding error.
   - Stopped: File creation stopped.
4. Click **Close** to exit the **Media Files** window.

To stop an ongoing transcoding:

1. Go to **Media > Transcoding**.
2. Click a media file of the status **Transcoding** or **Waiting**, and then click **Stop-transcode**.
3. Click **OK,** and then click **Close**.

You cannot stop transcoding files of the status **Error** or **Stopped.**

To restart a transcoding:

1. Go to **Media > Transcoding**.
2. Click a media file to be restarted, and then click **Re-transcode**.
3. Click **OK,** and then click **Close**.

You cannot restart transcoding for files of the status **Transcoding** or **Waiting**

System Administration

System Upgrade and Fallback

You only can upgrade or downgrade RealPresence Capture Server between RealPresence Capture Server versions. Upgrading or downgrading between RealPresence Capture Server and Polycom RSS 4000 is not supported.

- You can upgrade your system from 1.7 to 1.8 directly. If your software version is older than version 1.7, you need to upgrade your system to 1.7 first, then upgrade your system to 1.8.
- After system upgrade from 1.7 to 1.8, you need to re-activate the system using an activation key.
- Before you upgrade or downgrade your system, you should always back up your settings and recordings. Polycom is not responsible for any user data loss during these operations.

To update your system software to the latest version:

1. Go to **Admin > System Upgrade**.
2. View the license info and agree to them.
3. Click **Add** and select the version 1.8 software upgrade package, then click **Open**.
4. When asked to confirm the action, click **Yes**.

   The system uploads the package and performs the upgrade automatically. This may take several minutes.
5. Upon completion of the upload, click **Upgrade**. The system restarts to apply changes.
6. Enter your administrator **User ID** and **Password** and then click **Log In**.

   To confirm that the system is upgraded, check the software version on the **Product Activation** page.

System Fallback

Before system upgrade, the system creates a restore point automatically and after system upgrade, you can restore both image data and system configuration settings that existed at the time the snapshot was created

To fall back the image, configuration and IVR messages

1. Go to **Admin > System Fallback**.
2. Read the risk of system fallback and agree to it
3. Click **Fallback Capture Server**.

4 Click **OK**. The system restarts to apply the changes.

Fall back the system early as possible if you find it necessary after system upgrade, otherwise user data of the following operations will not be saved.

System Log Configuration

The logger utility is activated at the system startup and continually records system events. The log files generated by the utility contain the following information:

- Events occurred in system internal modules.
- Administrator activities.
- System login attempts.
- Operation errors.

All log files generated the day before are automatically compressed into a ZIP file named year-month-date.tar.gz at log maintenance window every day. The log maintenance window is usually the first hour from 00:00:00 system time every day. The log file storage is 30GB. You are prompted when the system reaches the storage limit. The system will delete the old logs to free the disk space at log maintenance window.

Configure Log Settings

You can change the system logging strategy, configure warning limit, and enable remote logging.

To configure the log settings:

1 Go to **Admin > Log Settings**.

2 Configure the following settings:

- Logging Level: Specify the system logging level, which decides to what level system events should be written into the center/server.log file.
  - **Info** – logs all non-debug messages.
  - **Debug** – logs all messages.
  - **Error** – logs the fewest number of messages.
  - **Warning** – logs between error and Info messages.
- Logger Warning Capacity: Specify the percentage of log file capacity used at which the system displays a warning on the dashboard.
- Log retention period (days): Defines the number of days to keep log archives on server.
- SysLog Server IP Configuration: To configure the IP settings of the SysLog server.

Log Management

The following table shows actions administrators and auditors can perform.

Log Management

Action	Description
Refresh	Refreshes the list and adds newly generated log files.
Download	Downloads the selected log file.
Download Today's logs	Downloads all the log files generated today.

To download log files:

1. Go to **Admin > System Logs**.
2. In the **Log** list, select the log to be saved.
3. Click **Download**.

Restart and Shut Down the System

You can shut down or restart your system.

Before unplugging RealPresence Capture Server, you need to shut down the server in Admin Portal.

If your RealPresence Capture Server does not restart after reboot or upgrade, you need to unplug your RealPresence Capture Server, wait for about five minutes, plug in your RealPresence Capture Server, and then reboot.

To restart the Capture Server system:

1. Go to **Admin > Restart/ShutDown**.
2. Read the risk of restart and click **Restart Capture Server**.
3. Click **OK** at the prompt message.

To shut down the Capture Server system:

1. Go to **Admin > Restart/ShutDown**.
2. Read the risk of shutdown and click **Shutdown Capture Server**.
3. Click **OK** at the prompt message.

Backup and Restore System Configuration

You can back up and save the system configuration of RealPresence Capture Server system to your local computer so you can restore the system configuration in case of necessary. Supported configurations include:

- **Hard Disk Warning Threshold**

- **IP setting parameters**
- **System time**
- **Recording Settings**
- **Certificate, port and security policy**
- **Gatekeeper, SIP, and QoS Settings**

To back up current system configuration:

1. Go to **Admin > Config Backup/Restore**.
   The configuration file will be stored on the local machine that the browser is running on.
2. Click **Backup**.

To restore the system configuration using the configuration file:

1. Go to **Admin > Config Backup/Restore**.
2. Click **Add**, select the .ppm file from local machine and click **Open**.
3. Click **Upload**.
4. Click **Restore**.
5. Confirm to restart the system.

Back Up and Restore Media Files

The RealPresence Capture Server system is able to backup media data to the FTP server in the network, and restore system user data to the selected media data snapshot (based on the time points generated in the backup). You can back up the entire media data. RealPresence Capture Server only uses passive mode FTP to transfer files.

Configure an FTP Server for Backup

Before backing up user data, you need to configure FTP server on the RealPresence Capture Server system first.

The RealPresence Capture Server system supports the following FTP servers:

- 3CDaemon
- FileZilla Server
- Serv-U
- Microsoft FTP7.x For IIS
- vsftpd

To automatically back up archives after call (Automatic Archive):

1. Go to **Admin > Data Backup/Restore.**
2. Select **Enable Automatic Archive**.

3 Configure the following settings for both FTP server and alternate FTP server.

FTP Server Parameters

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to save your media files.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to user root directory.
Password	
Use Anonymous	When this is enabled, you can log in to the FTP server using anonymous account.
Enable SSL	Set whether to enable SSL encryption for the communication between the RealPresence Capture Server system and FTP server. The system can only support implicit SSL FTP.
Test	Test whether the FTP configurations work.

4 Finish **Alternate FTP Server Configuration** if needed.

5 Click **Update**.

Once this function is enabled, archives could be transferred to configured FTP server and removed from local disk after call, this is achieved automatically.

Manage Archives and Live Streams Using the User Portal

The RealPresence Capture Server provides User Portal for you to view live streaming, play back archives and dial out for recording.

Your access depends on the type of account you use to log in. The archives, and live streaming may vary, depending on how archive permission is configured.

To log in to the User Portal:

1. Open a web browser.
2. In the browser address line, enter the system's portal address, for example, **https://System IP**

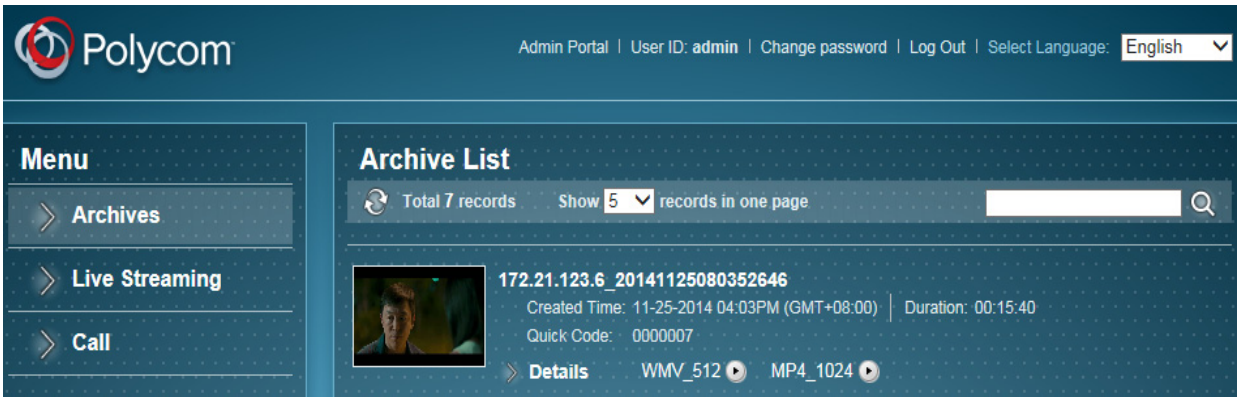
   Note: When an IPV6 address is used, refer to the following format: `https://[ipv6]`
3. Click **Log In** at the upper right of the screen.
4. Do one of the following:
   - Enter your user ID and password, then click **Log In**.
   - To log in as a guest, click **Anonymous Access**.

- You need to go to **Configuration > Portal Settings** and clear **Disable view permission of user portal for guest user.**
- If the Capture Server system is configured with an Active Directory server, users defined on the Active Directory can log in to Capture Server system with their AD account.

To switch to the Admin Portal from the User Portal:

1. In the address line, enter the system's IP address in this format: https://<system IP address>/.
2. Click **Admin Portal**, and then enter your user name and password to log in to the system.

RealPresence Capture Server User Portal



You can view live streaming and play back archives from the User Portal.

To view archives and live streams, your device must turn off the pop-up blocker. For example:

- For iPad: From **Settings > Safari**, make sure the option **Block Pop-ups** is **OFF**.
- For Android devices: From **Browser > Settings > Advanced**, make sure the option **Block Pop-ups** is **OFF**.
- For PC Internet Explorer (versions 9, 10, and 11): From **Tools > Internet Options > Privacy**, make sure the option **Turn on Pop-up Blocker** is NOT selected.

Manage Archives

From User Portal you can view details of archived files, search archives and play an archived file.

To view archive details:

» Click **Archives**.

To view the detailed information of the media files, click **Details**.

To search archives:

1. Click **Archives**.
2. In the search field at the upper right of the screen, enter the search phrase and then click .

To clear the search result and return to the full view, clear the search phase, and click again.

To play back archives through the User Portal:

1. Log in to the User Portal.
2. Go to **Archives**.

3 Select the archive you want to play back and click .

4 A new window opens to play the video.

If the e-mail notification function has been enabled for the VRR that is used to record archives, the system sends you an e-mail notification automatically once all archives have been converted and are ready for web playback. For more information, see Manage Archives .

If your web browser is the Internet Explorer, you may be prompted **Display mixed content?** When you view a live streaming. Click **Yes** to proceed.

This happens because the User Portal uses secured HTTP (http yet the streaming URL doesn't. You can change the Internet Explorer's default security settings from **Internet Options > Internet > Custom level > Miscellaneous > Display mixed content > Enable**.

View Live Streaming

You can now view live streaming from the User Portal.

To view your live streaming from the User Portal:

1 On a device with compatible web browser, open a supported web browser. See table "User Portal Web Browser Requirement" for the supported web browsers.

2 In the browser address line, enter the system's portal address, for example, **https://System IP**.

3 Click **Live Streaming** from the menu on the left.

4 Click the **Play** button of the live streaming that you want to play.

The live streaming is opened in a new window.

Call

You can start point-to-point recording or dial our from the Capture Server system through User Portal.

The **Call** menu is only available after you are logged into the User Portal.

To start point-to-point recording from User Portal

1 In the address line, enter the system's IP address in this format: https://<system IP address>/portal.

2 Enter the non-admin user name and password to log in to the system.

3 Click **Call**.

4 Click **2 Sites Recording** and enter addresses for two invited participants.

5 Click **OK**.

Dial out from Capture Server through User Portal:

1. Access Capture Server User Portal by its IP address or host domain name from a compatible browser.
2. Enter the non-admin user name and password to log in to the system.
3. Click **Call > Dial out to record**.
4. Configure the relevant settings.
5. Click **OK**.

Dial out to record is also available under **Call menu from Admin Portal**.
The recording starts immediately if **Start Recording Immediately** is enabled in the selected recording template.
For more information, see Configure VRRs .

Appendix A – Console Commands

RealPresence Capture Server supports essential system configuration by using Console. You can access Console via VGA or SSH, some popular applications like Putty supports SSH.

Login Console

The login interface shows all of the software information and you'll be prompted to enter the login password. Enter the login password and press the **Enter** key.

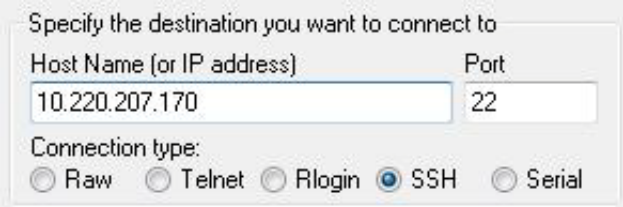
The factory default login password is polycom (case sensitive).

If you entered a wrong password, you may be required to re-login to the system.

If you entered the right password, you are brought directly to the command setting interface.

To log in to Console via SSH

1 Open SSH client, enter **Host Name** and **Port** (the default SSH port is 22).



2 Enter the user name and password (both are **polycom** by default)

Polycom
Polycon RealPresence Capture Server
Copyright 2010-2013 Polycom, Inc. All Rights Reserved.
Device Network Information:
eth0[192.168.1.254]
eth1[]
Use a supported browser to configure/manage this Polycom RealPresence Capture Server:
http://192.168.1.254
Use a supported telnet client to configure/manage this Polycom RealPresence Capture Server:
192.168.1.254

If you have completed all the above configurations and launched Console successfully, press the **Enter** key. The login interface appears.

Console Command Descriptions

You can use the following commands.

Network Settings

Select **Network Setting** and type **Enter** to set network configurations (DHCP IP address and static IP address) for LAN 1 or LAN 2.

To configure Static IP Address for LAN 1 or LAN 2

1. Choose a network interface, click **OK** or type **Enter**.
2. Select **Static Address Setup**, click **OK** or type **Enter**.
3. Configure network settings.

Parameter	Description
IP Address	IP address of the network port
Default Gateway	Gateway address of the network port
Subnet Mask	Subnet mask of the network port

4. Click **Save configuration** if you are fine with the settings or **Cancel** to return.
5. The system will show the prompt message *Yes to save the configuration?* Choose **Yes** to proceed or **No** to cancel.
6. At the popup message, click **Yes** if you want the system to restart to apply your changes.

To configure DHCP IP Address for LAN 1 or LAN 2

1. Choose a network interface, click **OK** and type **Enter**.
2. Select **DHCP Address Setup**, click **OK** and type **Enter**.
3. Click **Set To DHCP**.
4. The system will show the prompt message *Yes to save the configuration.* Choose **Yes** to proceed or **No** to cancel.
5. Click **Yes** if you want the system to restart to apply your changes.

After you set the connection feature or IP address for the LAN interface, the system must be restarted in order for the new settings to take effect.

6. Choose **DNS Server** and type **Enter** to configure DNS server address for the system to resolve domain names.

Disk Usage

Choose **Disk Usage** and type **Enter** to view the disk space usage of RealPresence Capture Server.

The total, used, and free disk space are shown.

Reset Console Password

This is to reset the console password, the system will show the prompt message to set new password to access console.

Reset Portal Admin Password

This is to reset the Portal Admin password, the system will show the prompt message to set new password to access the Admin Portal.

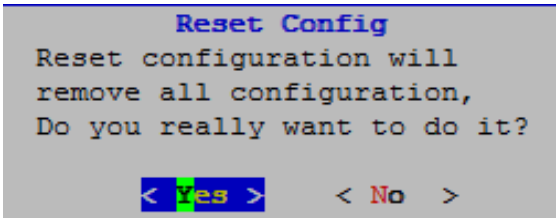
Reset Config

This is to reset the following system configurations to the default value:

- System Config
  - Call Settings
  - Signaling Settings
  - Port Settings
  - System time
  - Media Storage Settings
  - Multicast Settings
  - Certificate Management
  - QoS
  - SNMP
  - Active Directory

  - Password Settings
  - Customization
  - Portal Settings
- Admin
  - Log Settings
  - License
- Template
  - Recording Templates
  - Transcoding Templates
  - VRRs
  - Events
- Server
  - IIS
  - WOWZA
  - Windows Media Server
  - AKAMAI
- User
  - User
  - Group

The system will show the following prompt message



Click **Yes** to proceed or **No** to cancel.

After resetting the system configuration, the system must be restarted in order for the new settings to take effect.

Ping

Choose **Ping** and type **Enter** to check the network connection status.

Reboot

Choose **Reboot** and type **Enter** to restart the system. The system will show the prompt message *Do you really want to reboot the machine?* Choose **Yes** to restart the system, or **No** to cancel.

Shutdown

Choose **ShutDown** and type **Enter** to power off the system. The system will show the prompt message *Do you really want to shutdown the machine?* Choose **Yes** to restart the system, or **No** to cancel.

Fallback

Choose **Fallback** and type **Enter** to restore the system to the time the snapshot was created.

Click **Yes** to fall back the system or **No** to cancel.

Show

Choose **Show** and type **Enter** to show the general system information including System Version, Interface Information, and IP Address Information.

Exit

Choose **Exit** and type **Enter** to exit the command control interface.

Appendix B – Configure 3rd Party Media Servers

You can now stream live meetings and on demand meeting archives to leading 3rd party media servers, such as Wowza, IIS Media Service (Smooth Streaming only) and Windows Media Server. This feature expands the streaming audience capacity of the RealPresence Capture Server system.

Users can watch these streams and on demand meeting archives hosted on external media servers from within the Admin Portal, or from the User Portal.

For more information about Capture Server and Media Manager integration, see the *Integration Guide* from support.polycom.com.

On the RealPresence Capture Server system, you can live stream recordings and push VoD recordings to the following external media servers:

- IIS Media Server
- Wowza Media Server
- Windows Media Server
- AKAMAI CDN

You can view the live streaming or archives from the User Portal of the RealPresence Capture Server system.

The section shows some useful examples to configure third party external media servers, for latest configuration details, refer to third party external media server documentations.

Configure the Wowza Media Server

You need to configure an Wowza media server and your RealPresence Capture Server to work with the server as well.

1 Install JDK and Wowza. Run

`<Wowza directory>\examples\installall.bat` to create the needed configurations and directories.

Wowza Media Server Configurations and Directories

Parameter	Live Streaming	VoD
Application Name	live	VoD

Application Directory	<Wowza directory>\applications\live	<Wowza directory>\applications\vod
Configuration File Location	<Wowza directory>\conf\live\Application.xml	<Wowza directory>\conf\vod\Application.xml

2 To enable Wowza authentication, modify the configuration file as follows:

- For live streaming: Open `<Wowza directory>\conf\live\Application.xml`, set digest as the value for the tag `PublishMethod`. That is, `<PublishMethod>digest</PublishMethod>`.
- For VoD: Open `<Wowza directory>\conf\vod\Application.xml`, Polycom recommends you not to set authentication, make sure `playmethod` is none, `<PlayMethod>none</PlayMethod>`
- Open `<Wowza directory>\conf\publish.password`, type the your user name and password.

3 Install and configure a FTP server. The FTP server shares the <Wowza directory>\content directory. You need to grant you at least the **Read, Write**, and **Create Directories authorities**.

The following example shows the configuration for a FileZilla FTP server.

4 Start the Wowza server. When you see the message **Wowza media server is started!**, the server is started successfully.

To configure the RealPresence Capture Server system for working with the Wowza server:

1 Go to **Server > WOWZA.**

2 Click **Add**.

3 Configure the following basic settings

Wowza Server Parameter

Parameter	Description
Server Name	Specify the name of your **Wowza Media Server**.
Server Address	Specify the Wowza server IP address.
Server Port	Specify the port the Wowza Media Server used to receive live streaming. The value is 1935 by default. **Note:** Valid port values range from 1-65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server.

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

Enable Live Streaming

Parameter	Description
Streaming Protocol	Choose between **RTSP streaming** and **RTMP streaming.**

Application Name	Specify the name of the Wowza server application to be used for the live streaming. It should be consistent with the Wowza server configuration. In this example, application name is *live*.
User Name	Specify the user name to access the Wowza media server. This option is required when Wowza authentication is enabled. The **User Name** should be consistent with your input in To configure the Wowza server:
Password	Specify the password to access the Wowza media server. This option is required when Wowza authentication is enabled. The **Password** should be consistent with your input in To configure the Wowza server: .
Test	Test whether the live streaming configurations work.

5 Specify whether to stream video on demand (VoD) from this server.

- Application Name: the name of the Wowza server application to be used for the VoD.

  It should be consistent with the Wowza server configuration. In this example, application name is *VoD*.

6 When **Enable Vod is selected,** configure the following settings to transfer generated recordings to the Wowza server content directory:

Enable VoD

Parameter	Description
FTP Address	Specify the IP address of the Wowza server.
FTP Port	Specify the port assigned to the Wowza server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
Enable SSL	Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the FTP server.
Test	Test whether the FTP configurations work.

7 Click **OK**.

- You cannot create two external servers with the same Server type, IP, Port, and Application Name. This is because the RealPresence Capture Server system does not allow publishing two streams to the same publish point to avoid overwriting the first stream by the second one.
- External latency time will be introduced when external media server configured, compared with live streaming from Capture Server, the exact time varies depending on streaming protocol.

To create a VRR for use with an external server:

1. Go to **Template > VRRs**.
2. Click **Add**.
3. Configure the following settings:
   - VRR Name:
   - VRR Number
   - Description
   - Recording Template
   - Transcoding Template
   - e-mail Address: select this option and enter one or several e-mail addresses. Separate several addresses with commas (,).

     The streaming link is contained in the e-mail notification when the streaming is ready for viewing
4. To configure the rest of the settings, refer to the this user's guide.
5. Click **OK**.

Configure the IIS Media Server

You need to configure an IIS media server and your RealPresence Capture Server to work with the server as well.

When you configure an IIS media server, you can create two virtual directories, which are used for live streaming and VoDs.

To configure the IIS media server:

1. Launch the IIS manager, then create a virtual directory named as *live*, with the default port as 80. Specify the physical path for the virtual directory, for example, `C:\inetpub\wwwroot\live`.
2. Set the authentication methods.
   a. Select *live*.
   b. Double click **Authentication**.
   c. To play live streams on an iPad, make sure **Anonymous Authentication** is selected. To control an IIS publishing point from your RealPresence Capture Server make sure that **Windows Authentication** is selected.
3. Navigate to `C:\inetpub\wwwroot\`, create two `xml` files: `clientaccesspolicy.xml` and `crossdomain.xml`.

If you have installed the Polycom RealPresence Media Manager and IIS on the same server, you need to put the correct crossdomain.xml and clientaccesspolicy.xml files to the root directory of the RealPresence Media Manager portal.

For configuration steps, refer to Capture Server and Media Manager Integration Guide.

Here is the example text for the `clientaccesspolicy.xml` and `crossdomain.xml` files.

- clientaccesspolicy.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<access-policy>
<cross-domain-access>
<policy>
<allow-from http-request-headers="*">
  <domain uri="*" />
  </allow-from>
<grant-to>
  <resource path="/" include-subpaths="true" />
  </grant-to>
  </policy>
  </cross-domain-access>
  </access-policy>
```

- crossdomain.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<access-policy>
<cross-domain-access>
<policy>
<allow-from>
  <domain uri="*" />
  </allow-from>
<grant-to>
  <resource path="/*" include-subpaths="true" />
  </grant-to>
  </policy>
  </cross-domain-access>
  </access-policy>
```

4. Configure a virtual directory for VoDs if you want to play the archives through an IIS Media server.
5. Create a virtual directory named as *vod*, with the default port as 80. Specify the physical path for the virtual directory, for example, `C:\inetpub\wwwroot\vod`.
6. Install and configure a supported FTP server. The FTP server shares the VoD physical path, for example, `C:\inetpub\wwwroot\vod`.
7. Grant the users at least the Read, Write, and Create Directories authorities.

To configure the RealPresence Capture Server system for work with the IIS server:

1. Go to **Server > IIS**.
2. Click **Add.**

3 Configure the following basic settings.

IIS Media Server Parameters

Parameter	Description
Server Name	Specify the name of your IIS Media Server.
Server Address	Specify the IIS server IP address.
Server Port	Specify the port that the IIS server used to receive MP4 live streaming. The value is 80 by default. **Note:** Valid port values range from 1 to 65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server.

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

Enable IIS for Live Streaming

Parameter	Description
Application Name	Specify the name of the IIS server application to be used for the live streaming. It should be consistent with the IIS server configuration. In this example, the application name should be live.
User Name	Specify the user name to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.
Password	Specify the password to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.
Test	Test whether the live streaming configurations work.

5 Specify whether to stream video on demand (VoD) from this server. If enabled, also configure the following settings:

- Application Name: the application name to access the IIS media server

6 When **Enable Vod** is enabled, configure the following settings to transfer generated recordings to the IIS media server content directory:

Enable VoD for IIS

Parameter	Description
Application Name	Specify the name of the IIS server application to be used for the live streaming. It should be consistent with the IIS server configuration. In this example, the application name should be live.
FTP Address	Specify the IP address of the IIS media server.

FTP Port	Specify the port assigned to the IIS media server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
Enable SSL	Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the FTP server.
Test	Test whether the FTP configurations work.

7 Click **OK**.

You cannot create two external servers with the same Server type, IP, Port, and Application Name. This is because the RealPresence Capture Server system does not allow publishing two streams to the same publish point to avoid overwriting the first stream by the second one.

To configure a template and VRR for use with the IIS server, see To create a VRR for use with an external server:

Configuring the Windows Media Server

You need to configure an Windows media server and your RealPresence Capture Server to work with the server as well.

To configure the Windows Media Server:

1 Open Windows Media Services on program menu.

2 To enable Windows Media Server authentication, modify the properties as the following:

- .Navigate to **Server > Properties > Authentication**, make sure "**WMS Anonymous User Authentication**" is enabled.
- Navigate to **Server > Properties > Authentication**, make sure **"WMS Publishing Points ACL Authorization"** is enabled, and the Everyone user has full permission.
- For live publish point, RSS can create the live publish points, so don't need to create it manually at **Windows Media server**.
- For vod publish point, Create a On-demand publish point, input publish point name, location of content, for example, c:\WMpub\WMarchive.

3 Install and configure an FTP server. The FTP server shares the c:\WMpub\WMarchive directory. You need to grant the user at least the **Read, Write,** and **Create Directories** authorities.

To configure the Capture Server system for work with the Windows Media server:

1 Go to **Server > Windows Media Server**.

2 On the **ACTION** panel, click **Add**.

3 Configure the following basic settings.

External Media Servers Parameters

Parameter	Description
Server Name	Specify the name of the external server.
Server Address	Specify the IP or DNS of the external server you selected.
HTTP Port	The default value is 80.
RTSP Port	The default value is 554.

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

Enable Live Streaming

Parameter	Description
User Name	Specify the user name to access the external media server.
Password	Specify the password to access the external media server.
Test	Test whether the live streaming configurations work.

5 Specify whether to stream video on demand (VoD) from this server. If enabled, specify the application name. The application name is the name of the media server's application to be used for VoD.

Contact the administrator of the external media server for the naming rule of the application name.

6 When **Enable Vod** is selected, configure the following settings to transfer generated recordings to the pre-installed FTP server of the external server:

Enable VoD

Parameter	Description
Publishing Point	Specify a publishing point for Windows Media Server.
FTP Address	Specify the IP or DNS of the external server's FTP server.
FTP Port	Specify the port assigned to the external server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.

Parameter	Description
Enable SSL	Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the FTP server.
Test	Test whether the FTP configurations work.

7 Click **OK**.

Appendix C – Configure the Server Working with VCS

This chapter demonstrates how to configure RealPresence Capture Server working with Cisco TelePresence® Video Communication Server (Cisco VCS). The configurations are different between H.323 and SIP.

- Configure VCS for H.323 Calling
- Configure VCS for SIP Calling

Configure VCS for H.323 Calling

For H.323, after you register RealPresence Capture Server to the Cisco VCS, Cisco VCS works as a gatekeeper. you can configure the Cisco VCS and then call a VRR created on RealPresence Capture Server to start a recording.

To configure VCS calling:

1. Create authentication accounts in VCS, such as ff1/1234, ff2/1234….ff6/1234.
2. Register RealPresence Capture Server to VCS. See To register the system to a gatekeeper to make H.323 calls: for detailed steps.
3. Go to **Configuration > Signaling Settings** and set **Gatekeeper type** as **Cisco VCS.**
4. Register an endpoint to the VCS. For example, register Polycom Group Series 500 to the VCS.

Now you can dial from the Group Series 500 and the format of the address is `E.164+VRR Number`. After the call is set up successfully, you can check the RealPresence Capture Server Admin Portal.

Configure VCS for SIP Calling

If your network supports SIP, you can use SIP to connect to conference calls. Cisco VCS works as a SIP server.

To configure VCS for SIP calling:

1. Register RealPresence Capture Server to VCS via SIP. See To configure the SIP settings: for detailed steps.
2. Register an endpoint to the VCS via SIP. For example, register HDX 4000 to the VCS.
3. Configure the VCS to enable SIP calling.
   a. Log in to the Cisco VCS as an administrator.
   b. Go to **VCS Configuration > New zone** to create a new zone.

c Configure the zone for your RealPresence Capture Server. Refer to the following table.

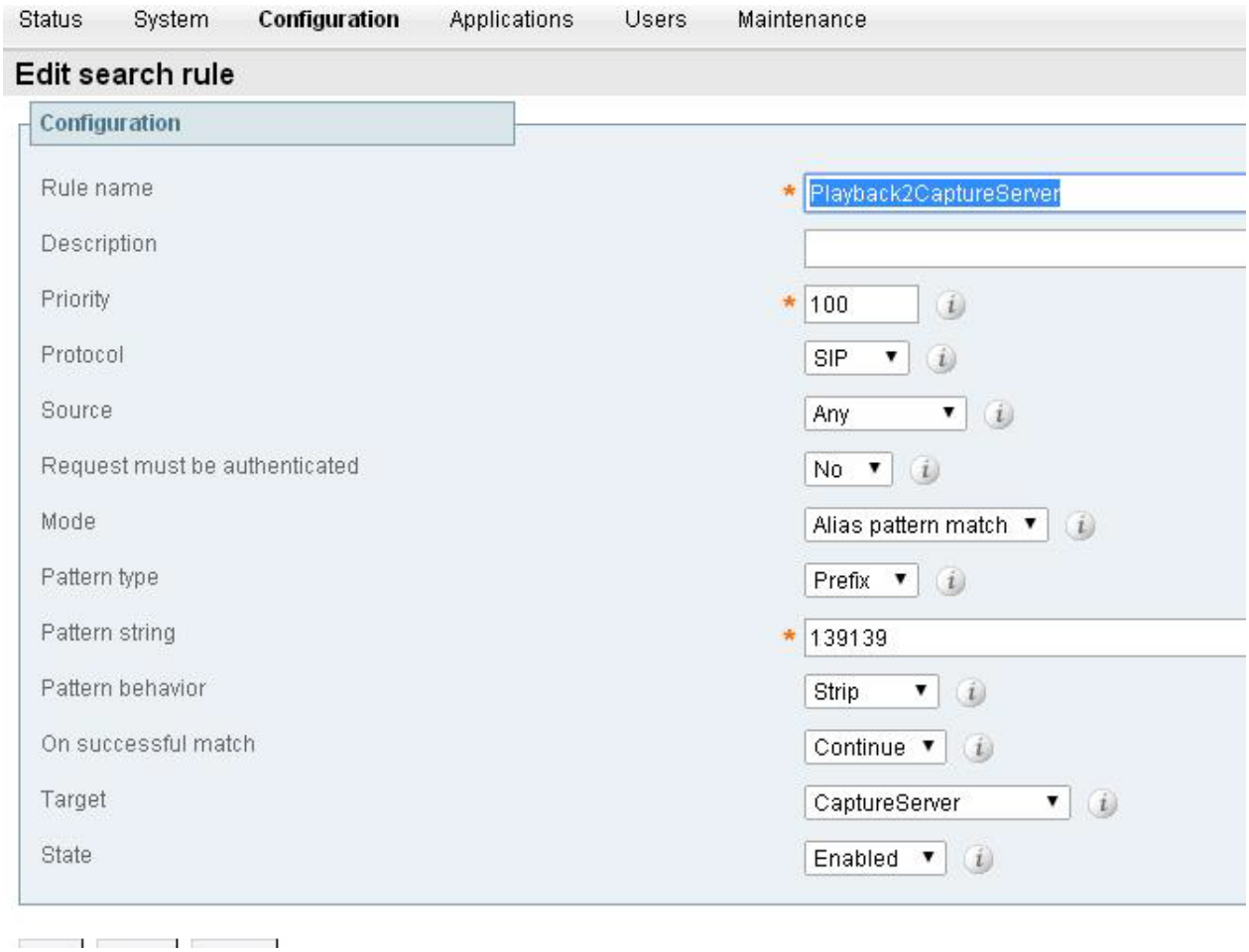
VCS Zone Parameters

Parameter		Settings
Name		capture_server_zone
Type		Neighbor
Hop count		15
H.323	Mode	On
	Port	1719
SIP	Mode	On
	Port	5060
	Transport	TCP
	Accept proxied registration	Allow
Authentication policy		Do not check credentials
SIP authentication trust mode		Off
Peer 1 address		Your RealPresence Capture Server IP address.
Zone profile		Custom

d Create a search rule to route to the zone you created.

The following example assumes that you have the default tandberg recommended rules in place.

Set search rule parameters



Now, you can start a recording by calling a VRR number from any endpoint registered to this Cisco VCS. For example, if the VRR number is 12345, you can dial *13913912345* directly to start a recording. 139139 is the prefix name (pattern string set in above picture).